Defining the Information within Military Information Operations: Utilizing a Case Study of the Jammu and Kashmir Conflict

A Monograph
by
Major Joe Daniels Bookard
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 05-06

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM- YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
25-05-2006	MONOGRAPH	SEPT 2005-MAR 2006

4. TITLE AND SUBTITLE		5a. CONTRACT NUMBER
Defining the Information within Military Information Operations: Utilizing a Case Study of the Jammu and Kashmir Conflict		
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
MAJOR Joe Daniels Bookard	
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
School of Advanced Military Studies 250 Gibbon Ave Ft. Leavenworth, KS 66027	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
Command and General Staff College 1 Reynolds Ave Ft. Leavenworth, KS 66027	CGSC, SAMS
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The current operating environment requires the United States military to conduct military information operations throughout the conflict spectrum, during all phases, and across various military operations. A function of the U.S. military is to deter adversaries who oppose the will of the U.S., and if unsuccessful, render them incapable of physical resistance, thus ultimately altering their behavior. In essence, the U.S. military wishes to alter tangible and intangible variables in any system to gain an advantage. As the U.S. military increases its reliance on information and its supporting infrastructures, the threat will continue to become more sophisticated, clandestine, and complex. Therefore, military commanders and their staffs should develop sophisticated approaches to describe, classify, and then explain essential elements within the information environment, particularly when conducting counterinsurgency operations (COIN).

The research presented in this work examines the Indian government's response to counterinsurgency through the categories of information defined by the author. The author's definition of information focuses on how decision-makers, mainly military commanders, assign value to information within and extracted from the information environment. The definition is an attempt to add clarity to the broad meanings found in the FM and JP 3-13 doctrine for Information Operations

15. SUBJECT TERMS

Information, Information Operations, Jammu and Kashmir, COIN

16. SECURITY CLASSIFICATION OF:			17 LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)	(U)	63	19B. TELEPHONE. NUMBER (Include area code) (913) 758-3300

Standard Form 298 (Rev. 8/98)

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Joe Daniels Bookard, USA

Title of Monograph: Defining the Information within Military Information Operations: Utilizing a Case Study of the Jammu and Kashmir Conflict.

Approved by:

_____   Monograph Director
David Burbach, Ph.D.

_____   Director,
Kevin C.M. Benson, COL, AR   School of Advanced
                                                  Military Studies

_____   Director,
Robert F. Baumann, Ph.D.   Graduate Degree
                                                  Programs

ABSTRACT

Defining the Information within Military Information Operations: Utilizing a Case Study of the Jammu and Kashmir Conflict by Major Joe Daniels Bookard, US Army, 63 pages.

The current operating environment requires the United States military to conduct military information operations throughout the conflict spectrum, during all phases, and across various military operations. A function of the U.S. military is to deter adversaries who oppose the will of the U.S., and if unsuccessful, render them incapable of physical resistance, thus ultimately altering their behavior. In essence, the U.S. military wishes to alter tangible and intangible variables in any system to gain an advantage. As the U.S. military increases its reliance on information and its supporting infrastructures, the threat will continue to become more sophisticated, clandestine, and complex. Therefore, military commanders and their staffs should develop sophisticated approaches to describe, classify, and then explain essential elements within the information environment, particularly when conducting counterinsurgency operations (COIN). The commanders' analysis of the information environment is critical and will be challenged by anonymous adversaries, and their remote geographic locations and access points coupled with inexpensive "off the shelf," simple technology. These factors require a significant demand for accurate and reliable information for mission planning and execution for combat operating forces.

The research presented in this work examines the Indian government's response to counterinsurgency through the categories of information defined by the author. The author's definition of information focuses on how decision-makers, mainly military commanders, assign value to information within and extracted from the information environment. The definition is an attempt to add clarity to the broad meanings found in the FM and JP 3-13 doctrine for Information Operations.

TABLE OF CONTENTS

TABLE OF FIGURES

GLOSSARY OF TERMS

The various terms used throughout this monograph are in Appendix A**.**

INTRODUCTION

The Information Operating Environment

Those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations.

-Sun Tzu, The Art of War[1]

The current operating environment requires the United States military to conduct military information operations throughout the conflict spectrum, during all phases, and across the various ranges of military operations. Sun Tzu's ultimate objective was to subdue the enemy without fighting. As early as 500 B.C, Sun Tzu's statement of fighting war without physical contact clearly depicts the military information operations capabilities of deception, disruption, and operational security. Additionally, it is clear that information advances will continue to affect how and with whom the U.S. fights wars. Furthermore, military actions involving the rapid advancement of information systems and infrastructures will shape the existing paradigm of war by kinetic means to one of understanding that information "in war" is a continuation of that paradigm. If war is a type of political conflict, then in theory, war in a non-physical state can exist as conflict over the interest embedded in politics, which is information. Information existing in tangible and intangible forms within the information system allows for influence, and creates power, which in turn produces a set of behaviors. The change in behavior can signal a transition point of success or failure in altering that system's tangible or intangible attributes.[2] A function of the U.S. military is to deter adversaries who would oppose the will of the U.S., and if unsuccessful, make them incapable of physical resistance, thus ultimately altering their behavior.

---

[1] Sun Tzu, *The Art of War*, translated by Samuel Griffith, (New York: Oxford University Press, 1971), 147.

[2] The author defines tangible is those physical properties of a system and intangibles as non-physical properties. The tangible elements include concrete or touchable items that emit signals. Intangible elements are just the opposite; they are immaterial, elusive, or insubstantial items.

As the U.S. military increases its reliance on information and its supporting infrastructures, the threat will continue to become more sophisticated, clandestine, and complex. Therefore, military commanders and their staffs should allow sophisticated approaches to describe, classify, and then explain essential elements within the information environment, particularly when conducting counter-insurgency operations (COIN).[3] The commander's analysis of the information environment is critical; with a clear understanding of this environment the commander is better able to predict challenges from anonymous adversaries, using remote geographic locations with anonymous world-wide-web access points, coupled with inexpensive "off the shelf" technology.

Information requirements represent the information that is pertinent to the users in terms of content, accuracy, and format.[4] To understand how information affects the ability to perform military operations, it is necessary to define what information is and to think about information as existing in three dimensions: physical, information, and cognitive.[5] Each of these three dimensions is addressed in a later section, but the importance them for military decision-makers involves understanding where information lies within each dimension , how it is extracted and employed as a weapon or defense, and how it is used to form perceptions. Operations in Iraq and Afghanistan demonstrate the challenges of the cognitive dimension of human nature in warfare. Regardless of what means the military uses to defeat an enemy in battle, kinetic destruction will not affect some elements within the information and cognitive dimension. Those areas may be intangible in nature, difficult to detect, and maybe transmitted as unorganized signals and thus be excluded from the commanders decision-making process.[6] The difficulty is the threat system

---

[3] The author's definition of information assists in classifying information within the COIN information environment.

[4] Whitten, Jeffery, Lonnie Bentely and Kevin Dittman. *Systems Analysis and Design Methods.* Sixth ed. (Boston, MA.McGraw Hill Companies, 2004), 237.

[5] David Alberts, et al. *Understanding Information Age Warfare*. (U.S., DOD Command and Control Research Program, 2001), 12.

[6] Ira G. Wilson and Marathann E. Wilson. *Information, Computers, and System Design*. (John Wiley and Sons, New York: 1967. "Unorganized Signals" are those patterns of communication not easily recognized by the receiver from the sender until some form of interpretation occurs.

adapts to either an organized or an unorganized pattern that continues to emit information, which places the military decision-maker at a disadvantage. A classification system of these elements of information can mitigate unwarranted risk when U.S. forces are involved in COIN or operations other than war.

The common understanding of information is that it is about the transmission of signals between senders and receivers, or the message or media as Arquilla's definition suggests on page 16, but the author's research presented in this paper suggests an understanding that information exists at the core of all existence. Biological and social systems have information at their core, and their motion, behavior, and evolution all revolve around information processing.[7] The author's definition of information on page 18 will suggest that all systems (tangible and intangible) contain embedded information. The embedded information creates an organized or unorganized system. A restructuring of incoming signals from the information environment occurs before information is processed and or transmitted. This may seem to suggest that "everything is information" but rather it suggests "everything has information" embedded in it if it has structure.

Information operations are of increasing importance to military commanders, as they consider employing lethal and non-lethal effects on the battlefield to exploit or degrade the threat's ability to fight. The commanders' ability to employ capabilities is directly proportional to the staff's ability to decipher information received from or remaining within the information environment. This is critical because information is how commanders command and control forces, establish objectives, and make decisions.[8] Information operations will continue to serve as a way to gain

---

[7] John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (RAND, 1997), 442. Information processing notes the ability of a living system to process matter and energy to maintain them counter to entropy.

[8] Charles Eassa. *U.S. Armed Forces Information Operations – Is the Doctrine Adequate?* (Fort Leavenworth, Kansas. Student Monograph, 1999), 5.

intelligence and knowledge to improve friendly operations, but denying the adversary the opportunity to employ similar capabilities is also important.

Structure

This monograph describes the use of military information operations in COIN by combining existing concepts of information theory in an effort to organize the elements of each into categories of information. After stating the research problem and limitations, a discussion of the value of using India as a case study will follow. The next two sections beginning on pages 10 and 16 will define the terms information and military information operations (IO). Specifically, they will examine what information is, how information sources collect and assign value to the raw data, and why information is so important in the Jammu and Kashmir counterinsurgency. After presenting existing definitions of information, the author will define and classify information into two categories: ideal information sources and information source changer.[9] The basis of classifying information comes from its tangible and intangible properties within a system. The next section beginning on page 23 will review and compare current DOD and Joint Publications of military IO to further clarify and combine previous discussions of information and the categories of information and military IO. This will assist in classifying the U.S. military IO capabilities into the two categories of information: ideal information sources and information source changer. These two categories will assist in classifying information operations activities, and will be used later to examine COIN operations within the Jammu and Kashmir conflict. The following sections beginning on pages 36 and 50 describe the historical context of the Jammu and

---

[9] The term ideal information source definition is on pg. 20. However, throughout the paper its use is interchangeable between the physical and cognitive dimensions. The term source describes those tangible and intangible origins of information. It can serve as an informer or cause to collect tangible and intangible data. As we struggle to combat and win a Global War on Terror (GWOT), with a transnational enemy who shares, in some cases, only a common ideology (intangible). Those intangible elements within the environment may present useful data that require further investigation. Yes, some form of information exists within everything. The military planners challenge is accurately identifying the elements within the information environment that meets the commander's intent and achieves his end state.

Kashmir conflict, then use the two categories of information to classify and explain India's COIN plan. The final section (page 58) presents a summary of findings for operational level planners to consider when categorizing information.

Statement of the Problem

The primary research question of this monograph is: Can a revised definition of information and its framework derived from existing information theories inform operational level military planners conducting COIN? This paper examines existing concepts of information and provides a definition of information that takes into account the tangible and intangible information variables. The expanded definition of information when applied to a case study of the Jammu and Kashmir COIN effort assists operational level planners in classifying information within the information environment. This categorization of information should provide the operational level planner an understanding of the various forms of information affecting decision-making, the importance of information operations in COIN, and the value of information operations India uses to conduct containment operations against insurgents in Jammu and Kashmir.

Limitations

This monograph does not attempt to change existing U.S. IO doctrine, but seeks to inform planners of how foreign IO concepts and their employment of intangible variables are similar to U.S. IO methods in COIN operations. The monograph will examine and compare U.S. IO capabilities (Civil-Military and Psychological Operations, Public Diplomacy and Physical Destruction Operations) with the Indian IO activities, to consider which capabilities had the most effect in India's COIN operations. This paper will not discuss other service doctrine or publications concerning information operations.

Although India has not officially released its concept of information warfare, the planning assumption made for this research is that their IO activities are the same or parallel with U.S. IO doctrine.[10]

The Value of Using India as a Case Study

The next section describes the relevance of using India as a case study, and provides the reader the background associated with the conflict in Jammu and Kashmir. The value of using India as a case study in evaluating IO activities in COIN is evident in two factors. These factors include India's ability to identify the threat, and India's use of public diplomacy to denounce and limit the threat's ability to conduct operations.

The classification of the insurgent groups and their political and military performance capabilities can serve as the basis for analysis for the collection and analysis of information. Bard O'Neill, an author in insurgent and revolutionary warfare, spoke of seven types of insurgent movements – anarchist, egalitarian, traditionalist, pluralist, secessionist, reformist, and preservationist.[11] The first factor is India's accuracy in classifying its insurgency as secessionist. The secessionist type of insurgency does not recognize the existing political community, but seeks to create a new one. Based on India's analysis of their insurgency in Jammu and Kashmir, India considered at least three options to counter the insurgents: 1) negotiate with the insurgents, 2) employ state armed forces or and 3) request international support to help restore legitimacy to the government of India if the Indian military could not do so. In India's case, the insurgent's goal was not to overthrow the existing form of state governance, but to alienate itself from the established set of state rules, thus forming an independent state. The insurgent goals allowed

---

[10] Several classified documents suggest that their capabilities are similar if not the same as U.S. IO doctrine. Additionally, this assumption is based on the open-source publication and planning guidance for U.S. IO.

[11] Bard E. O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare* (Dulles, VA: Brassey, Inc, 1990), 17. Bard O'Neill is a leading author in theories of insurgency and revolutionary warfare.

India to impose state legislation in conjunction with military and paramilitary forces to contain the insurgency in Jammu and Kashmir, thus making it a problem for the state of India, which required no international assistance.

The second factor India used to defeat the threat was to use public diplomacy as a defense to denounce any involvement of external/internal support to the insurgents, followed by imposing state legislation to de-legitimize them. India was publicly declaring its involvement in the War on Terror and needed no outside interference in dealing with its internal threats. This tactic allowed India to create an atmosphere or perception that the Pakistani government was an external supporter of its state insurgency; this also allowed India to gain international approval and assistance if requested in the Global War on Terror.[12] Whether these claims of Pakistani external support are true, the point is that after India's information operations, either Pakistan had to support India in defeating the insurgency or Pakistan would receive scrutiny by the international community regarding the support of the insurgents

India, unlike the U.S., uses its IO capabilities domestically as well as internationally. The domestic application of COIN combined with activities of military IO would pose judicial and moral challenges within the U.S. The scope of those challenges is beyond this monograph, but the research will examine the important capabilities within the Indian information warfare plan, which parallel U.S. information operations, and can inform military operational level planners.

Indian COIN operations against the suspected Pakistani insurgent organizations are helpful to illustrate the various means to combat terrorists using military information operations. Those means include psychological operations, civil-military operations, and physical destruction. For more than 50 years, Pakistan and India have fought three wars over Jammu and Kashmir. Of these wars, two were over Kashmir (1948 and 1965) when Pakistan attempted to take control and

---

[12] Excerpt from *The Truth about Kashmir and Terrorism in India*. (U.S. State Department Report on Terrorism, 2001).

liberate the people from the secular state of India. India has been involved in a counterinsurgency operation in the area from 1947 to the present. Terrorism has claimed more lives in India than anywhere else in the world, with more than 100,000 persons killed in various parts of the country. The insurgency has caused an estimated 400,000 displaced Kashmiri Hindu who became refugees of the state; 30 total active insurgent organizations; and about 600,000 Indian military forces deployed in support of Kashmir.[13] Terrorism in its contemporary phase started in 1978 in Punjab, India although Indian communal and ethnic violence has been ongoing since its independence in 1948.[14] The rise of contentious politics between different groups within India based on ethnic, racial, linguistic, and other divisive criteria is the root cause of many of the secessionists.[15]

Kashmir is one of the most important challenges in promoting stability throughout the South Asian region. The perception of U.S. intervention in Kashmir would be one of support to Pakistan, especially if ongoing U.S. operations for al Qaeda terrorists in Pakistan and Afghanistan help to end the activity of insurgents in Jammu and Kashmir.[16] India continues to claim that the dispute over Kashmir is a domestic issue and any interference from the Pakistani, U.S., or international organizations in handling its insurgency would be in violation of its national sovereignty. Although no known terrorist groups are operating within India that directly pursue an anti-U.S. agenda, the U.S. has included the Jammu and Kashmir terrorists in the U.S. Foreign Terrorist Organization Exclusion list, signifying a concern of national interest.[17] India's position on Jammu and Kashmir conflict does present a U.S. national security concern for the stability of the South Asian region for two reasons. First, with a U.S. concern that both India and Pakistan

---

[13] Paul Mendhurst, Global *Terrorism*. (United Nations institute for Training and Research Programme of Correspondence Instruction, 2002), 10-25.

[14] Yonah Alexander, *Combating Terrorism: Strategies of Ten Countries*. (Ann Arbor: The University of Michigan Press, 2002), 301.

[15] Ibid, 302.

[16] Kaia Leather, *Kashmir Separatists: Origins, Competing Ideologies and Prospects for Resolution of the Conflict* (Hauppauge, New York: Novinka Books, 2003), 4.

[17] DOS *Foreign Terrorist Organization Exclusion List Dated 2004*. Available at www.state.gov/s/ot/rlsks/37191.htm.; accessed 1 January 2006.

have tested nuclear weapons in 1988, ongoing-strained diplomatic relations between the neighboring states and the tension in Jammu and Kashmir may escalate to a point of nuclear exchange.[18] Secondly, Pakistan has become central to the global war on terrorism, and many believe that the dispute in Kashmir energized by Islamic terrorists creates added tension between the Hindus in India and the Muslim society, mainly in Pakistan. The U.S. Congress views the ongoing human rights violations in India as a U.S. national security issue, and assumes that both Islamic terrorists and Indian security forces in Kashmir are allegedly participating in these human rights violations.[19]

In summary, the U.S. has stated it will assist any international partners' capacity and capabilities to defeat terrorists and to promote human dignity and rule of law across the globe.[20] This statement is critical in gaining coalition support to conduct protracted warfare. The effort that India has undertaken to defeat its insurgency Jammu and Kashmir has maintained the region's stability between India and Pakistan.[21] The analysis of a long duration counterinsurgency allows planners multiple approaches in identifying how decisions and tactics evolved over time, and how the decision-maker conveyed intent through policy and military means.

The next section defines information from three perspectives: DOD, engineering systems design, and contemporary authors. The combination of these terms will assist in building the author's definition of information.

---

[18] Kia, *Kashmir Separatists*, 3-7.
[19] Kia, *Kashmir Separatists*, 3.
[20] United States of America, *National Defense Strategy, III Desired Capabilities and Attributes, Key Operational Capabilities*, 2005.
[21] Grau, Lester. *Kashmir: Flashpoint or Safety Valve*: Military Review, (July-August 1999), http://fmso.leavenworth.army.mil/documents/kashmir/kashmir.htm. (21October 2005).

DEFINING INFORMATION

This monograph suggests a revised definition of information for military purposes due to the lack of specificity in the current FM and JP 3-13 (Information Operations) doctrine. Although the doctrine articulates the concept of information operations, it does not fulfill its mandate by establishing a common understanding of the term information and the value of other dimensions of information. This point is of particular interest when conducting COIN operations, as information exists in tangible and intangible forms connected to human behavior and decision-making. The analysis of an insurgency forms the basis of most COIN strategies, and the analysis's development begins with what motivates the insurgences, what comprises its strategies, the nature of the insurgents' environment and the capabilities of the threatened government. Successful insurgencies occur when the "will" of the insurgents is greater than the "will" of the local populace and its state's response. In order for a military commander to measure the success of COIN operations targeting the insurgents "will," which is intangible, the commander must assign some value to the information collected prior to conducting COIN operations.[22] The value placed on this intangible information (will of the people) assists military planners in anticipating relationships internal and external to the insurgent group. Without a clear definition of information, a commander and his staff may not draw complete inference to the information attached to human nodes, influence links, religion, and nationalism. The next three sections of this paper will define terms in relation to existing concepts of information and information theory and then combines them to form the author's definition of information.

The United States Government (U.S.G.) considers information as one of the elements of national power, and military commanders conduct information operations to apply this power in a military operation. Modern information technology and the reliance on this technology is

---

[22] Celeski, Joseph. *Operationalizing COIN*. JSOU Report 05-2 (Hurlbert, Florida: The JSOU Press, 2005), 17-21, 31, 39, 42.

spreading information faster and wider than ever before.[23] The organizations or military

commanders who are able to recognize changes in information technology and capitalize on them

by shaping the preferences of organizations or systems around them exert power.[24] Although this

power is intangible, it is still measurable by changes in an organization's system of behavior, by

its internal and external interaction, and the degree to which a system adapts within the

organization. The application of military information operations in a system through core, related

and supported capabilities exerts this form of power.[25] A detailed discussion of these IO

capabilities will occur in a later section.

Department of Defense Joint Publications 1-02 and JP 3-13

This section will use the DOD and Joint Publication definitions of information to assist in

building the author's definition of information. Additionally, an understanding of the difficulty in

defining the term information is useful. A clear articulation and coherent understanding of the

term information will help planners consider appropriate operations with supporting resources

that are within their organizations' capabilities.

The Department of Defense (DOD) JP 1-02, provides two definitions of the term information.

The first describes information as "facts, data, or instructions in any medium or form." The

second meaning of information described by the JP 1-02 is what a "human assigns to data by

means of the known conventions used in their representations."[26] Expanding this definition, the

DOD requires conditions to create information dominance as articulated in the Joint Vision 2020,

"Information Superiority." Information dominance is effectively transmitting the right form of

---

[23] Nye, Joseph S. Jr. *Soft Power: The Means to Success in World Politics*. (New York: Public Affairs, 2005), 1.

[24] Information system has the characteristics and ability of an organization to collect, analyze and disseminate information.

[25] Will be addressed in a later section

[26] Department of Defense, JP 1-02, Dictionary of Military and Associated Terms (Washington, D.C: U.S. Government Printing Office, 2001), 202.

information in time and space to the correct system.[27] The medium or form is similar in meaning

to the "Information Environment" (IE) as described in the JP 3-13. Information within the

medium is can be either organized or disorganized: organized information is information easily

translated or interpreted into usable information for the decision-maker. On the other hand,

unorganized information may contain redundancies in transmission signals, differences in signal

variations or addresses that may seem jumbled or confused. An example of simple organized and

unorganized information is e-mail, which is a message created and transmitted via a "signal," and

that signal contains both the message and information. If the sender has the correct signal,

Internet Protocol and e-mail address, he sends organized information. The signal becomes

unorganized when either the IP or the e-mail address is incorrect. The value of the original

message begins once an uninterrupted signal is established.

The IE consists of three dimensions of information- physical, information and the cognitive

dimension.[28] The physical domain is where the information environment overlaps with the

physical world. Computer networks, populations, communication nodes and supporting

infrastructure that allow transmission characterize this region. In a military context, the physical

dimension is where the situation the military seeks to influence exists. The physical dimension

allows for the application or employment of means to achieve a desired diplomatic,

informational, political or economic end state. The systems in the physical dimension are the

easiest to measure, and historically equate to combat power measurements.[29] Within the

information dimension are the creation, transmission, storing, and manipulation of information

systems. Information links the physical and cognitive dimensions together and allows the

military commander to convey his intent, command and control, and flexibility to execute

military information operations. In reality, the ability of information technology to change an

---

[27] Joint Vision 2020, Chairman of the Joint Chiefs of Staff, Director for Strategic Plans and Policy. (Washington , D.C.: U.S. Government Printing Office, June 2000).

[28] JP 3-13 July 2005 draft description of the Information Environment.

[29] Alberts, *Understanding Information Age Warfare*, 12.

organization has little to do with technology and everything to do with how the organization is able to leverage the inputs from the information and physical dimensions into the organization's systems.[30]

The last IE dimension in the JP 3-13 is cognitive, "the mind."[31] This dimension is where creative thought, decision-making and visualization happens. This dimension includes the minds of the adversary as well. Perceptions, personal experiences, training, world-views, and individual capabilities all form the lens for the cognitive dimension. Consequently, the challenge associated with this dimension is the perception of reality.[32]

In summary, the DOD publication identifies three dimensions of information: physical, information and cognitive. Unfortunately, the definition is limited to the military's application of physical force. Understanding the DOD definition of information with the enhancement proposed in this paper enables the building of an information definition and framework for understanding information operations in India's COIN operations. The next two sections highlight the various definitions and theories of information from engineering system organizations, and contemporary authors in the information theory profession.

Information as Part of a System Design

This section and the second definition of information come from principles of information and system design as applied in system engineering. It provides an engineering approach in understanding the definition of information, and its use in both tangible and intangible states. This approach to understanding information serves as the core of the commanders' collaborative information environment within the context of the author's research. Ira Wilson, a PhD in engineering systems design, definition of information and system design is to map out in the

---

[30] Alberts, *Understanding Information Age Warfare*, 12.
[31] Joint Publication 3-13. *Information Operations*, I-3.
[32] Alberts, *Understanding Information Age Warfare*, 13.

mind, to plan mentally, to conceive as a whole, completely or as an outline. Wilson defines input

stimulus or information as the agent, a form of molecular excitation that influences the actions of

the organization or system in whole or any part.[33] The term molecular, or cognitive dimension

described by DOD for the intended purpose of this research, describes the building blocks of

input stimuli and transmission leading to output stimuli.[34] In order for the human mind to

interpret the physical properties of the incoming transmission (from a sender) of information,

information is then converted into signals, which are manipulated into outputs based on the

interpretation or decision-making of the human mind.[35] That analysis of the conversion of

physical information properties into signals then converted into outputs forms the basis of the

ideal information source and information source changers discussed in the author's definition

section (pg. 17). During this process, expended energy in the form of information comes from

the exchange between the input and output systems; the value of that information is assigned by

the molecular system. The emphasis is on the role of the energy and structural aspects of

systems, particularly on the role human beings and information play in system design and

operation. Input stimulus flows from the source to the system in space but varies by time, and

must be in the form of energy. The information energy flow may be continuous over an interval

of time (as in speech) or interrupted (as in telegraph signals)."[36] Wilson stated output energy

changes a material object that exists in space and time from one state to another. This energy

flow is one way and is observable by the human mind that translates it into organized or

disorganized information.

   The conclusion here is that the design of a system is largely by the work of the human mind,

"the cognitive dimension," interacting with input stimuli forming information. The next section

---

[33] Ira G. Wilson and Marathann E. Wilson. *Information, Computers, and System Design*. (John Wiley and Sons, New York: 1967), 9.
[34] Ibid.
[35] Ibid, 14.
[36] Ibid, 15.

will present Arquilla and Ronfeldt's "Three Views of Information," which are helpful in further refining the authors meaning of IE and dimensions of information.

John Arquilla's "Three Views of Information"

The third definition considered comes from John Arquilla and David Ronfeldt, both RAND analysts, who presented views of information in terms of the inherent "message," the "medium" of production and storage, and as a "physical property or physical matter."[37] Information creates language that expresses ideas and joins concepts. Information as a message is without form but serves as a signal that contains some coherent content when transmitted from a sender to a receiver.[38] This type of message, when depicted in a physical state, is in the form of instructions or programs. Arquilla's second view of information is information in the form of a medium. He proposes that information is represented not only in the message, but also in the system or organization that transmitted the message to a receiver. These views suggest that the content is irrelevant and that what is important is the organization or system's ability to encode and transmit the message. As discussed in the section of information system design, this "exchange of energy" between the input "sender" and output "receiver" produces information.[39] This random complex exchange of energy produces both organized and disorganized messages and mediums, which increases the difficulty of assigning value to the information. The information concepts of message and medium are formless or immaterial but the last view of matter suggests that information encompasses both the physical reality and energy.[40] In discussion earlier, information exists between a sender and receiver's exchange and within the physical dimension,

---

[37] John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (RAND, 1997), 145.
[38] Ibid.
[39] Ibid, 145-146.
[40] Ibid, 148.

which is reality. Information and physical matter co-exists and forensics, biochemical functions and the central nervous system are all examples of physical matter with information.

In summary, the definition of information provided by DOD publications is similar to that of John Arquilla's "Three Views of Information," but differs in the packaging of transmissions and the form of information types. The definition from Wilson's Information System Designs is the link between the tangible and intangible elements of information. In the next section, the author's definition suggests that the military commander, based on his military end state and objectives, decides the value of information.

AUTHOR'S DEFINITION OF INFORMATION

This section presents the author's definition of information, and then presents an understanding that information is a source of power and is defined using three existing concepts and definitions. These particular concepts are critical in drawing relationships among the three dimensions of information previously discussed. The information concepts will come from the Department of Defense (DOD) definition of information, Ira G. Wilson's "information systems design construct" and John Arquilla's "Three Views of Information." The definitions from the existing lexicon, when modified, will create a framework for evaluating India's insurgents and the counterinsurgency plan related to information operations. The purpose for combining the definitions is to inform the reader of the importance of the intangible elements within the information environment. In order for the U.S. military to assist in "winning the hearts and minds" of people, the intangible value must be addressed by understanding the desired end state and the potential for uncertainty. In periods of uncertainty, if few courses of action are available, then information has little value if it does not eliminate uncertainty or allow for an interpretation within the affected system. Additionally, the value of information depends on the number of resources or activities that are able to collect, monitor and regulate the output of the required

information. This means the various sources collecting information must provide measurable

data to assess the quality or value to avoid an undesirable effect.

   This paper proposes a definition of information composed of the ideal information source and

the information source changer. This definition of information, as applied to this research

framework, is a modification of the previously discussed definitions and is stated as "a process of

the tangible and intangible elements of a system communicated or received concerning a

particular fact or circumstance."[41] This suggests that the understanding of the content occurs

initially between the sender "input" and receiver "output" sources, but expands once the

molecular system[42] identifies patterns and influences related to their reality. The tangible

elements include concrete or touchable items that emit signals. Intangible elements are just the

opposite, they are immaterial, elusive, or insubstantial items. Assigning meaning or values to

tangible or intangible elements starts with an existing database of knowledge. This database or

knowledge repository resides with the decision maker and the receiver of information. The

decision-maker[43] sets the stage by defining the overall problem and the initial scope and function

of the intended information to the information source. This allows the ideal information source to

extract information related to the requirements outlined by the decision-maker, or future

requirements not anticipated by the decision-maker.[44] In this context, information can be broken

down into two categories: ideal information sources and information source changers. These two

categories will serve as the proposed framework in understanding the complex nature of the

information environment within the Indian counterinsurgency in Jammu and Kashmir. Figure 1

depicts two categories of information with the related IO activities of CMO, PSYOP, and

---

[41] The author has a combined definition of information from DOD, Ira Wilson and Alberts.
[42] The decision-maker is the military commander or collaborative system that assigns the final value to organizations information.
[43] For the purpose of this monograph, the terms decision-maker and commander are interchangeable.
[44] Whitten, Jeffery, Lonnie Bentely and Kevin Dittman. *Systems Analysis and Design Methods.* 6th ed. Boston, MA.: (McGraw Hill Companies, 2004), 237 and 486.

Physical Destruction that were present in the Jammu and Kashmir COIN.

Categories of Information		Indian IW Capabilities		
		CMO	PSYOP	Physical Destruction
Ideal Information Source (source agent) - encodes signals and transmits information	Sensory inputs are a combination of the physical and cognitive dimensions. They provide direct observation and input into a system or organization. The content of this information or "ideal information source" is passed from human interaction, experiences (intuition), the worldview, public opinion or any perceive understanding about a system. Initial value and assesments of information occur here.	Provides information to support IO goals. Can synchronize media and PA messages ISO of CDRs Intent. Identifies supporters of military operations, and what infrastructure needs assistance.	Provides information decision-makers want the TA to be aware of. This information is generated from the physical and cognitive dimensions. Assest in establishing metrics for understanding future effects of IO activities.	Provides initial TA and objectives. Ensure success of military objectives. Ensures correct TA set is acquired and serviced.
Information Source Changer (source changer) - decodes signals from information environment and ideal information source	Influence is the ability to affect a person, thing, or course of events without any direct or substantial effort. Since the exchange between input and output produces energy, the secondary affect or influence on that system causes a slight deviation in the original organizations structure, that deviation is information. The value of that information occurs after the decision-maker reviews collected information from the ideal information source.	Provides news to local people and government. Incorporates COCAM to portray ground truth to proponents and opponents of operation. Assist government in establishing legitimacay and rule of law.	Assist PSYOP ability to purport themes and messages. Identifys individual, the enemy or other supporters of the enemy who may present challenge military operations. Shapes norms, attitudes and behaviors. These activities are based on the CDRs Intent.	May limit targeting and ability to convey PSYOP messages. IO capabilites of CNO, CI, and MILDEC all serve as measures to influence adversary decision-makers.

Figure 1 Two Categories of Information compared to Indian IW Used in COIN[45]

Figure 1 provides a description of ideal information sources and changers as types of information. It then draws a relationship between current U.S. IO activities of CMO, PSYOP, and Physical Destruction that is similar to India's IW concept, and highlights the salient point's key in COIN operations. Both the ideal information source and information source changer require inputs from the information environment, stemming from sensory inputs and or patterns. The various types of collection assets - inputs - help focus the collection effort on the perceptions, attitudes, and behaviors of the environment for the decision maker. The intelligence collection activities of the ideal information source are severely constrained to ensure compliance with the

---

[45] The chart above is the author's original work but includes some information from various open source publications.

law, but other agencies and law enforcement officials can supplement intelligence collection.[46] The chart shows no major changes to the meaning of IO capabilities when compared to the two information categories, but it does present a wider lens to view information within the information environment.

Ideal Information Source (Input)

The ideal information source is a combination of the physical and cognitive dimensions. The term source describes the physical and intangible origins of information. The ideal information source can serve as an informer or cause to collect tangible and intangible data. The information source provides direct observation, and intelligence for input into a system or organization. This information input provided by the ideal information sources comes from human interaction, experiences (intuition), the world-view, public opinion, or any perceived understanding about a system. At this point, the ideal information source processes, collects, and disseminates received signals from the IE, to an informed decision-maker aware of associated patterns and perceptions of the information. The ideal information source gathers information based on the scope, function and requirements assigned by the commander; his estimate allows information valuation to occur with the decision-makers.[47] Although the ideal information source assigns initial value to information prior to transmission to the decision-maker, this analysis is precursory. Information not supporting the commander's initial collection requirements, are documented and used to populate the commander's collaborative information environment. An example of this is how the commander articulates Commanders Critical Information Requirements (CCIR) or establishes High Value Individuals (HVI) for targeting and observation. The staff can then begin the staff estimate process and organize resources and activities to inform the commander of the

---

[46] The US CODE: Title 552, Public Information: agency rules, opinions, records, and proceedings, outlines the legal compliance for information collection and dissemination.
[47] Concept from Ira Wilson's *System Design*.

course of action he chooses to execute. The validation of the information requirement occurs when the ideal information source transmits to an informed decision-maker aware of the associated patterns and perceptions of the information within his collaborative environment. Global perceptions, personal beliefs, proponents and opponents of state actions, and Reuters are additional examples of ideal information sources. The CMO, PSYOP capabilities meet the requirements of ideal information sources used in the Jammu and Kashmir COIN operation, and are discussed in a later section.

The ideal information sources can determine potential partners, groups, or organizations associated with insurgents and the ideal information source can identify potential opponents or third parties through whom to coordinate in order to inform the decision-maker which threat may be detrimental to the collection or can influence the process. Their initial collection should focus on achieving the military objectives that mitigate risk and possibly build coalition support within the local populace. Understanding that the information the ideal information source collects from the information environment, mainly the cognitive dimension, is the individual's perception and governed by the individual's interpretation of laws. This makes the application of desired intangible effects difficult to measure as this information exists within the information environment for some receiver.

Information Source Changer (Output)

The other classification, the information source changer, produces influence and patterns. Since the exchange between input and output produces information, the secondary effects are influence and patterns. The information source exchange identifies the target audiences' beliefs, attitudes, and behaviors after the decision-maker assigns a value to the collected information. As noted earlier, this information produces both organized and disorganized messages and allows the receiver to interpret them. Influence as a category of information incorporates elements of the

physical and cognitive dimensions within the information environment. The spiritual and moral values used by the Kashmiri insurgents' exercises indirect command over the local populace in the region. In this particular case, influence comes from the various interpretations of the meaning of their religious writings. Influence can represent cause and effects that appear independent, but when integrated with ideal information sources can establish patterns of behavior that determine the outcome of a situation. This is evident by the ethnic violence in the primarily Muslim-dominated Kashmir, where the belief that a complete Muslim state will exist and all of the actions conducted by the insurgents lead toward that goal. Observing how the insurgents influence the populace through tangible and intangible means can present a solution to deescalate tension within Jammu and Kashmir, or provide input to the decision-maker's information database. Examples of influence are individual perceptions, adversaries, sympathizers, and minds of the nation supporting the defending state, or the minds of the state supporting the enemy. This is important to remember, because the information environment includes tangibles and intangible information. The deterrent power of nuclear weapons is an example of influence.

In understanding that the information environment is collaborative, the IO activities of Civil-Affairs, PSYOP and physical destruction all provide influencing types of information. The CMO produces and promotes legitimacy of operations and communicates the "good news" to the local populace. Psychological operations assist in communicating the overall message and help shape the local populace perceptions and beliefs about on-going military operations. Additionally, PSYOP and CMO can limit the physical destruction targeting effects of non-combatants by conveying accurate messages and by measuring patterns of behaviors within the area.

A coherent definition of information suggests it is impossible to predict the nature of a system and associated events; however, it is possible to interpret, change and analyze data within the information environment and assign value during the decision-making process to produce the

greatest effects on military forces. With the majority of U.S. doctrine available through open source channels via the World Wide Web, printed and broadcast media, potential adversaries have made detailed studies of U.S. capabilities and will seek to degrade those capabilities by operating around U.S. technology.[48] The decisive factor in future conflict maybe determined by the speed and accuracy of a sophisticated or unsophisticated opponent's ability to interpret information. This evidence suggests that technology has given both sides the opportunity to understand the battlefield and target vulnerable areas within the military system. Some of these targeted vulnerabilities affecting both the U.S. and its opponents are the media, rules of engagements and the complex relationships of alliances and coalition partners. These targeted vulnerabilities make system prediction impossible due to their linkage with internal/external agents.

The previous sections described the various meanings of information. It suggests that information is energy and can exist in any form. With the proper identification of information, it can enable or hinder a commander's ability to extend power. The definition of information established by the author, "information is a process of the tangible and intangible elements of a system communicated or received concerning a particular fact of circumstance,"[49] can suggest a broader meaning and is useful at the operational level.

The next chapter will review the capabilities of military information operations that build upon the U.S. Army's definition, the contemporary authors' definitions introduced in the paper, combined with the monograph author's definition of information to present a military information operations conceptual framework for categorizing information.

---

[48] Whitepaper on *Capturing the Operational Environment*, received from Mr. Walter Williams (Threat DCSINT) Fort Leavenworth, KS. This was an unofficial paper produced internally February 2, 2000.

[49] The author defines information as a process of the tangible and intangible elements of a system communicated or received concerning a particular fact of circumstance. This limits the understanding of the content initially to the sender "input" and output sources "receiver" but expands once the molecular system identifies patterns and influences related to their reality. In this context, information can be broken down into three categories: ideal information sources and influences.

MILITARY INFORMATION OPERATIONS

Through the analysis thus far, the reader should understand the various forms of information: how information is energy in the form of signals and how power can exist in the information. The next two sections will examine the U.S. Army's core, supporting and related IO capabilities utilizing two primary references, the FM 3-13 and the JP 3-13. The five core capabilities are psychological operations (PSYOP), military deception (MILDEC), operational security (OPSEC), electronic warfare (EW) and computer network operations (CNO). The five supporting IO capabilities are counterintelligence (CI), combat camera (COMCAM), physical attack, physical security, information security. The three related capabilities are defense support to public diplomacy (DSPD), public affairs (PA), and civil-military operations (CMO).[50] How one uses information will determine the existing capability to employ information and whether the information is useful or not. Additionally, the term information warfare is not part of the current joint IO doctrine. This change is part of the 30 October 2003 DOD Information Operations Roadmap that provides a common framework for understanding IO and policies and authorizes Combatant Commanders to integrate and execute IO.[51]

Military information operations are used to some degree in all ranges of military operations, from conventional to the emerging stability and support operations. The current Army field manual describes information operations as the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to affect or

---

[50] JP 3-13, Information Operations, pg. II-1.

[51] The DOD Information Operations Roadmap provides the Depart a plan to advance the IO as a core military competency. The roadmap articulates the importance of PSYOP in wartime

defend information and information systems, and to influence decision-making.[52] Joint

Publication 3-13 defines information operations as:

> actions taken to affect adversarial and others' decision making, attitudes,
> behaviors, information systems, and information while protecting our own
> through the integrated employment of the core capabilities of electronic warfare,
> computer network operations, psychological operations, military deception, and
> operations security, in concert with specified supporting and related capabilities
> throughout the information environment.[53]

The first core capability is PSYOP. These operations intend to convey selected information

and indicators to foreign audiences to influence their emotions, motives, and behavior of foreign

governments.[54] The conducts of PSYOP is a large part of how the U.S. influences foreign

audiences to elicit behaviors favorable to U.S. objectives and are "the only operations authorized

by the DOD to influence the target audience through the use of media, print, broadcast, and other

media related outlets."[55] Psychological operators can produce themes and messages due to the

exposure they have with the local populace and can assist commanders in identifying patterns and

behaviors within the affected population.

Military Deception includes actions planned and executed by commanders that deliberately

mislead adversarial decision makers as to friendly military capabilities or intentions.[56] The

purpose is to encourage the adversary to use or gather incorrect information and to draw invalid

conclusions from the perceived information.

Operations Security, the third IO core capability, closely relates to MILDEC. The difference

is that OPSEC denies the adversary the ability to gather information to assess friendly capabilities

---

[52] FM 3-13 (FM 100-6), information operations: Doctrine, tactics, techniques, and Procedures, (November 2003)
[53] JP 3-13, Introduction.
[54] Ibid.
[55] Ibid.
[56] Ibid, II-3.

and intentions.[57] Operations security is critical in the information environment. Due to the speed

of information processing and interpretation, the security requirements of the sender and receiver

are changing constantly due to the adaptability of agents within an existing system. This security

is necessary in the physical, information and cognitive dimensions of information. As discussed

earlier, the value of information is based on an individual assessment and occurs after the receiver

analyzes the information based knowledge or from observable experiences. Through this

analysis, it can be determined what information is valuable and what is not. The challenge here is

the receiver's ability to recognize the value of both tangible and intangible information prior to

transmitting it to the decision-maker, because some discarded disorganized data may include

information needed for mission planning. The paper will present India's use of a similar concept

to the U.S. OPSEC in their COIN plan.

Electronic Warfare and CNO are the last two core IO capabilities. The fourth core capability,

EW, refers to any military action that uses electromagnetic (EM) and directed energy (DE) to

control the electromagnetic spectrum or to attack the enemy.[58] This warfare has three

subcomponents: the first is Electronic Attack (EA), which uses the EM or DE to attack, jam,

deceive, or destroy systems employed in a defensive nature. Second, Electronic Protect (EP) is

the protection of friendly capabilities against undesirable effects of adversarial employed EW.

The last subcomponent is Electronic Warfare Support (ES), which provides surveillance of the

EM spectrum and allows immediate recognition of the electro-magnetic threat.[59] All of these

subdivisions, when collaborated can produce signal intelligence (SIGINT), measurement, and

signature intelligence (MASISNT).[60]

---

[57] Ibid, II-4.
[58] Ibid, II-5.
[59] Ibid.
[60] Ibid.

Computer Network Operations and EW are those attacks that deceive, exploit, and defend electronic information and infrastructure.[61] These operations include computer network defense (CND), computer network exploitation (CNE) and computer network attack (CAN).[62]

Five supporting IO capabilities include information assurance (IA), physical security, physical attack, counterintelligence (CI), and Combat Camera (COMCAM). Information assurance provides protection of IO information systems and assumes that access to information is possible from inside or outside DOD controlled networks. The next two IO supporting capabilities are physical security and physical attack. Physical security protects physical facilities containing information and information systems and physical attack is the employment of other IO capabilities to influence target audiences. Counterintelligence and COMCAM are the last two IO supporting capabilities. Counterintelligence personnel guard information and its supporting systems, and propose initial adversary intelligence systems estimates. Computer Network Operations enable CI operations.[63] The COMCAM supports all capabilities of IO that use images of U.S. or coalition forces. They provide images for PSYOP, PA and CMO activities and although their products are sensitive,[64] the PA can release them to media organizations.

The last component of information operation capabilities are three related activities; Public Affairs (PA); Civil-Military Operations (CMO); and Defense Support to Public Diplomacy (DSPD). These sometimes-misunderstood activities must be coordinated with IO core and supporting capabilities to increase effectiveness of information operations. Public Affairs operations constitute public information, command information, and community relations

---

[61] Ibid, II-6.
[62] CND are actions taken to protect, monitor, and analyze unwarranted computer activity, CNA are actions through computer networks that disrupt, deny, degrade, or destroy information resident in computers and computer networks. CNE enable intelligence collection capabilities using computer networks to gather data from an adversaries automated information systems network.
[63] Ibid, II-9.
[64] Ibid, II-10.

activities intended for DOD and non-government organizations.[65] The PA function allows a consistent message or theme of operational matters pertaining to DOD activities to the target audience and internal organizations, preventing a loss of credibility. Additionally, PA, along with the media and COMCAM, can redirect negative perceptions, behavior and misinformation by the adversary through accurate and timely reporting. Civil-Military Operations establishes or exploits relationships between governmental, military, and nongovernmental civilian organizations[66] and extends the military commander's influence into areas where physical destruction creates more harm than good. The CMO activities are those that are normally the responsibility of local, regional or national government officials. The optimum time for CMO to occur is during the pre-hostilities phase or Phase 0, but they can occur at anytime.[67] The DSPD related capabilities are measures taken by DOD to facilitate public diplomacy efforts of the USG. They promote U.S. foreign policy objectives and shape counter drug, humanitarian relief, and global counterterrorism activities. India used a similar concept by portraying Pakistan as a state supporter of terrorists operating within their borders.

Information operations activities of Civil-Affairs, PSYOP, and physical destruction are the most closely related to the Indian information warfare capabilities (IW) conducted in their COIN operations. The three IO activities will serve as the ideal information source and sensory inputs for the decision-maker. Whether expressed in terms of U.S. IO activities or Indian Information Warfare capabilities, the two categories of information assist in classifying information across the full spectrum of operations.

This section's summary of military information operations and the previous section's definitions of information will enable a more useful understanding of the existing IO planning

---

[65] Ibid.

[66] Ibid, II-2.

[67] Civil Affairs teams, Special Operations Forces, PSYOP or conventional military forces perform CMO functions.

fundamentals. One of the concepts of IO is to collaborate with the different capabilities and

related activities to produce integrated effects, thereby possibly minimizing the need to employ

kinetic force in military operations. One sees this collaboration of IO activities by the

overlapping of core, supporting and related activities. The Information Operations Roadmap

previously discussed is the DOD aim of addressing perceived organizational shortfalls within the

DOD.[68] The primary focus of the document is to assign tasks regarding Public Affairs, Public

Diplomacy and PSYOP to improve cooperation between the White House and DOD regarding

Strategic Communications. Implementation of the roadmap is underway, but the challenge will

remain in the redundancy of overlapping functions and responsibilities of those IO capabilities.

Additionally, the current FM 3-13 and JP 3-13 do not mention IO themes or IO messages,

because none exist. However, there are PSYOP themes and messages and Public Affairs themes

and messages or "talking points" stated in the JP and FM 3-13.[69] In some ways, the creation of

generic IO themes and messages by local commanders can run counter to established U.S.

Strategic Communications messages or guidance within the commander's area of operations.[70]

Too often, the terms PA and PSYOP are misused. Public Affairs operations are truthfully

informing the public and unlike PSYOP do not focus on directing or manipulating public actions

or opinions.[71] The DOD doctrine provides guidance to staffs for the preparation and planning of

IO in support of operations, with the goal being to maintain an atmosphere of information

superiority for the U.S and its Allies.[72] The utility of information operations is in the

understanding that information is power, and in order for the U.S.G to maintain its status of a

"super power," it must have the ability to project power unhindered across the globe. The

---

[68] Report by the Defense Science Board Task Force on *Strategic Communication.*   (OUSD, 2004), 78-79.

[69] PA themes as related to IO capabilities, JP 3-13. II-8.

[70] Strategic Communications are those efforts focused specific audiences to create conditions favorable for strengthen, encouraging the advancement of USG interests. (JP 3-13, G12).

[71] DoDD 3600.1 (2001, 2).

[72] JP 1-02 defines Information Superiority as the operational advantage gained from the collection, process, and dissemination of uninterrupted flow of information while exploiting or denying the adversary the ability to do the same.

findings thus far suggest that information operations and the two categories of information serve as a means to assist planners to collaborate analytically within the information environment to identify the interaction of intangible agents within complex problems or uncertain empirical data.

The next section will present an overview of current U.S. IO planning fundamentals as described in the JP 3-13.

Current IO Planning Fundamentals

This section examines information planning fundamentals as understood in the JP 3-13 Chapter V entitled "Planning and Coordination," and how IO planners prepare for the execution of IO strategy. Although there are no planning fundamentals listed in the current FM and JP 3-13 IO doctrine, however the fundamentals listed in the JP 5-0 planning process collectively summarizes joint IO planning principles and processes.[73] This vagueness occurs in IO when tactical level IO objectives are not coordinated with the operational objectives. The strategic guidance and communications from the U.S.G. drive the formulation of interests and goals for a particular region. The President of the United States has charged STRATCOM with integrating IO core capabilities across the range of military operations. Combatant Commanders should then integrate, plan, and execute IO in support of the overall guidance established, thus synchronizing tactical and operational IO plans.

The fundamentals below ensure full integration of all staff sections and a common understanding of what is required of IO prior to the execution of an information strategy. A clear understanding of the national and strategic guidance, allows for complete understanding and articulation of the Joint Force Commander's mission, concept of operations and overall objectives. The correct identification of the adversaries' strategic and operational centers of

---

[73] The steps of joint planning include; initiate the planning, mission analysis, course of action (COA) development, COA analysis and war gaming, COA comparison and approval followed by plan or order development. Detail discussion of each component can be found inn the JP 5-0.

gravity and his vulnerabilities allow the planning effort to devise IO required tasks and subtasks. Planners during this stage should designate the organizations of subordinate forces and designate command relationships in order to plan and coordinate IO resources. The last point mentioned in the Joint Publication is the consideration of legal limitations as outlined in U.S. Code: Title 552, Public Information.[74] These planning fundamentals can guide planning and narrow the focus of the nation's strategic communications guidance into executable IO tasks at the operational level.

Information operations planning fundamentals begin by understanding the expectations and intent of national objectives. This allows planners to identify potential tasks early on that relate to IO and the potential role of IO capabilities. The early preparation allows prior coordination for employment of IO assets, intelligence preparation of the battlefield and the establishment of ownership for release authority of capabilities such as PA, MILDEC and CA activities. The legal considerations involving IO require examination of host-nation policies on information or information sharing, and the U.S. domestic constraints included in the U.S. Constitution. Standing U.S. laws set parameters on the employment of IO in the contemporary operating environment. Planners conducting the initial IO planning phase may identify related or major issues within the information dimensions that affect the problem. The planners should consider secondary events associated with the adversaries' influence network, and conceptualize the potential cause and effect linkages from the interactions of friendly and threat responses. This process occurs when information signals from the information environment pass via signals to the ideal information source, in this case to the IO planner. The IO planner assigns initial belief values and conducts estimates that inform the decision-maker in developing situation awareness. The planner's estimate helps establish or validate the commander's initial understanding of the problem, as well as issues needing investigation and key areas to influence.

---

[74] Summarized comments from the JP 3-13, V1-V7.

The next section will present an Information Operations framework that will examine India's COIN operations in a later section.

MILITARY COMMANDERS' INFORMATION FLOW

The last section examined how IO planners can prepare for executing an IO strategy. This section will move the process from planning to execution. Additionally, this section will describe the importance of the commander or decision-maker in analyzing received information and the ability to interpret information to develop it into his intent. The information principles used by Ira Wilson are helpful in categorizing the ideal information sources and the information source changer that produces patterns and influence.[75] The information source changer assists the decision-maker in placing value on information that leads to execution of assigned IO activities. The underlying principle allows for an understanding of how societies, culture, and systems communicate and make decisions using various types of information.

---

[75] See previous section of Information as part of a system on page. 15.

The illustration in Figure 2 incorporates the existing theories of information into one that categorizes information into two parts.
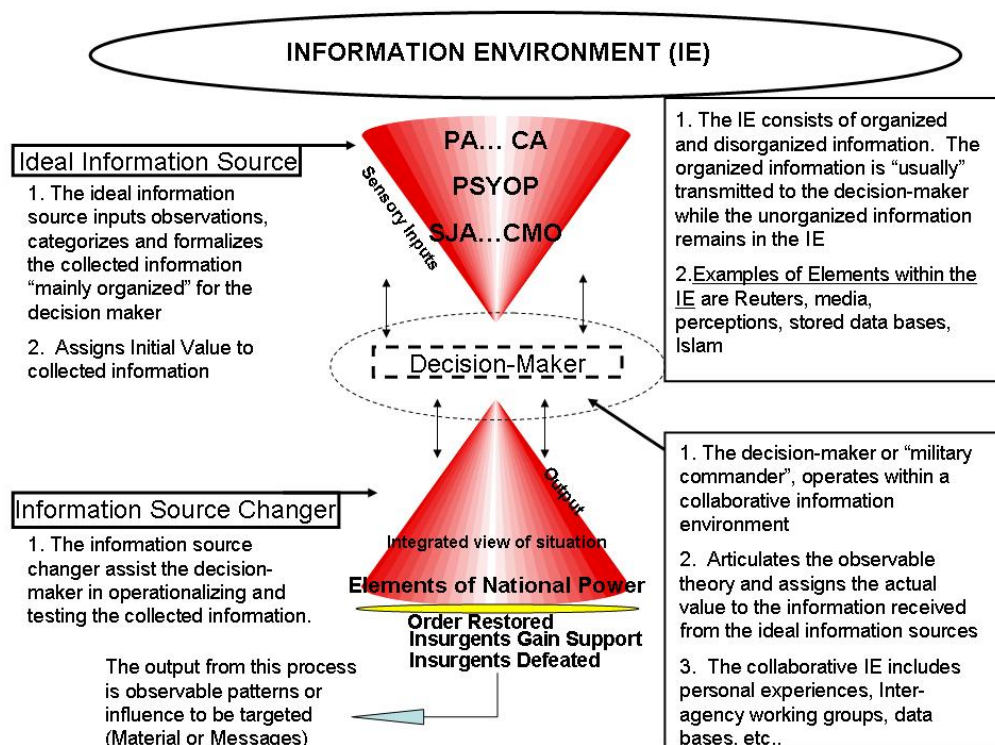

Figure 2 Conceptualization of Interpreting Information

The categories of ideal information sources and information source changers allow for the ease of grouping related IO capabilities during COIN as they pertain to the information environment. The framework does not account for the capability of intelligence, surveillance, and collection assets or the ability of those assets to process the information; it merely identifies those capabilities of IO best suited to conduct IO tasks. The ideal information source is the commander's conduit of information. The information environment provides the ideal information source messages in the form of signals. These messages come in various mediums and serve as tangible or intangible contributors to information. Some forms of messages include media, local populace, printed documents, and perceptions of religion, documented data sources, and proponents and opponents of the operation. The transmission of information goes to the molecular system; in this case, the molecular system is the military decision-maker. Information

can be transmitted through various input "sensors" which are part of the military's collection and analysis system that informs the commander on priority intelligence requirements and battle damage assessments from previous operations. As depicted in Figure 2, sensory inputs assist the commander in assigning value to intangible and tangible information that the source changers executes. The decision-maker defines the value of the information through the initial assessment given by the ideal information source and from within his information environment. The same variables that the ideal information source provided can exist across a spectrum of utility. The decision-maker is a molecular system, as in most hierarchical institutions such as the military. A filtration process of information signals passing through ideal information source channels occurs prior to receipt by the decision-maker. In Figure 2, the dotted lines represent the filtration of information prior to reaching the decision-maker. Although this filtration assists in framing the decision-makers problem, synthesis in most cases is lacking due to the experience level of the staff, environmental conditions, and inadequate collection focus by the ideal information sources.

The decision-maker's information environment includes interagency working groups, intelligence collaborators, and databases of behavior patterns of participating populations, independent research terrorist behavior networks, and analysts who create policy.[76] This area creates the synergy for the commander's decision-making process. Here, the commander has access to information in the physical, cognitive and informational sense, and controls the valuation of information from the ideal information source. Additionally, this point of convergence comes from other collaborative planners, historical predictive analysis, and other systems within the information environment. The decision-maker uses the input from the ideal information source to observe, categorize, or formalize the information into his overall intent and purpose for planning, execution, or collection efforts. After assigning value and articulating the information "intent," the decision maker transmits an organized signal to various subordinates

---

[76] Notes from Dr. Eric V. Larson RAND briefing on *Influencing the Desired Audience: Some Challenges and Approaches of Interest*. April 21, 2005 CAC IO Symposium.

where information conversion occurs, from intent to executable tasks. The medium the decision-maker uses to transmit signals to subordinate receivers is in the form of CCIRs, commander's guidance and intent statements or mission planning orders.[77]

Through shared experiences and training, the subordinate receivers execute the assigned decision-makers' intent previously identified and collected by the ideal information source. This facilitates command and control of subordinate forces and allows execution of information operations, which is the targeting of beliefs, values, attitudes, and behaviors. The true goal of IO is to allow a process that informs the commander of tangible and intangible characteristics within his COE and offer options to mitigate or exploit the effects of the information operations. This supports the purpose of IO in creating a psychological change in an adversary's system. Information operations occur after the decision-maker places value on the collected information and communicates that analysis to subordinates for execution. The subordinate receiver decides what IO activities are best suited to achieve the decision-makers intent by ensuring an integrated view of the situation. The subordinate informs the decision-maker whether the selected IO activities are accomplishing the intent and achieving the desired psychological effect. In Jammu and Kashmir COIN operations, CMO, PSYOP, and physical destruction IO activities assisted in restoring some pockets of order, and resulted in negotiated settlements with select insurgents.

The reader should understand that strategic communications is the integrating process that feeds into the information operations activities (PA and PSYOP), which promote the commander's messages and themes. This process integrates military capabilities with the information the military commander uses to make decisions in an effort to match a target audience identified by the U.S.G. The importance of this is a link from the information dimension to a common objective contributes to the success of the U.S.G. interests and policies.

---

[77] Signal is the medium of information that translate into organized meaning, i.e. Commanders Intent.

In summary, the information environment has both internal and external dimensions that affect every aspect of military operations from the initial planning, to the execution and consolidation phases. The decision-maker identifies the scope and function of the information needed for his problem analysis. Based on the initial requirements assigned by the commander, information is collected. This data is presented as estimates or analyses into the commanders' collaborative decision-making environment where the valued of information is assigned. The commander's collaborative environment includes other commanders, repositories of historical data, independent researchers and analysts, and interagency working groups. The commander and his staff evaluate and validate the information, and package it as guidance and tasks assigned to subordinates for execution.

Information operations can address the sociological, psychological, and economic conditions of the environment only if the content of the information environment and the ideal information source are able to decode each other's signals. Shortfalls within this system occur when the decision-makers and his collaborative information environment encounter a situation where the future deviates from past trends. Additionally the predictive powers of databases used by the decision-makers diminish with the increase of complexity within the information environment.[78] This promulgates an increase in the number of ideal collection sources, and the capacity or reliance of communication assets to account for the emergent behavior within the information environment.

The next two sections will provide a brief historical review of conditions that led up to the conflict over Jammu and Kashmir. The section will identify ideal information sources within the political, military, and social institutions of the Indian military. After the identification of the ideal information sources, this paper will examine Indian threats and their COIN plan utilizing the

---

[78] Notes from Dr. Larson brief during the CAC IO Symposium (April 2005).

two categories of information. The examination will describe India's IW capabilities of CMO, PSYOP and physical destruction effectiveness during the COIN.

THE CONFLICT IN JAMMU AND KASHMIR

History of India: Conditions That Led to Counterinsurgency Operations

This section will describe the historical context in India that led to the ongoing insurgency between Islamic Pakistan and Hindu India. The history highlights India's struggle for independence and the evolution of the political institutions in its society.

India has been a civilization since 2500 BC, and during the 4th and 5th centuries AD, northern India unified under the Gupta Dynasty. This period known as India's Golden Age and Hindu culture flourished. Islam spread across the subcontinent over a 500-year period. In 10th and 11th AD, the Turks and Afghans invaded India and established sultanates in Delhi. The Hindu Chola and Vijayanagar Dynasties in southern India dominated this century. Both Hindu and Muslim societies co-existed, leaving lasting effects on one another.[79] In 1619 at Surat, the first British outpost in South Asia was established; this expansion ultimately created division between the co-existing Muslims and Hindus of India.

The first true sign of conflict occurred when the British colonial rulers of India gave Prince Maharaja Singh rule of the state of Jammu and Kashmir in 1846. The area the British selected had a 70 percent Muslim population; the British failed to take into account the religion of Maharaja and his government officials, who were all Hindu. This lack of understanding of cross-cultural diversity and the history of religions added to the population's struggle with social justice and ignited several uprisings in India and the Kashmir regions. In 1857, a rebellion in North India led by Indian soldiers caused the British Parliament in 1885 to transfer all political power from East India Company to the British Royal family, allowing Great Britain to rule India

---

[79] Library of Congress – Federal Research Division; Country Profile: India December 2004

directly. The Indian National Congress, (INC) created in 1905, immediately began protesting

British rule in East and West Pakistan. Mohandas Gandhi transformed the INC into a mass

movement to campaign against British colonial rule. Eric Hoffer's (author of *The True Believer,*

presented arguments on the types of people who join mass social movements and their

motivations for joining) framework categorizes types of participants of mass movements into the

poor, misfits, outcasts, minorities, and adolescent youth.[80] The Hindu's Gandhi compelled to

protest British rule came from those particular categories Eric Hoffer described for starting mass

movements. The historical importance of the presence and voice of Mohandas Gandhi was that

he identified the injustices associated with social stratification within a politically and religiously

diverse society. Gandhi was the voice of the Indian people and was possibly the trigger for the

continuation of social conflicts to follow.

The insurgent groups within India are cross-cultural, but have one ideology in common, and

that is to see Jammu and Kashmir a free state. Unfortunately, with a British parliamentary system

of governance embedded into India's culture and a predominantly Hindu society, the country was

bound to implode. These reasons are the underlying factors of India's current state of insurgency.

The British parliamentary system influences India, and according to its constitution, it is a

"sovereign, socialist, secular democratic republic." Conflict between Hindus and Muslims led the

British to partition British India in 1947, creating the countries of India and Pakistan.[81] The

partition allowed individual states within the country to choose to align with Pakistan or India or

remain independent. During this process, the states of Hyderabad, Jammu and Kashmir, and

Junagadh remained uncommitted. Hyderabad and Junagadh joined India, and in 1947, the Hindu

---

[80] Hoffer, Eric. *The True Believer: Thoughts on The Nature of Mass Movements.* (New York, Harper Collins Publishers, 1951), 24-27.

[81] Library of Congress – Federal Research Division; Country Profile: India December 2004

Maharaja of the predominantly Muslim Jammu and Kashmir signed the Instrument of Accession to India after the invasion in 1948 of his territory by Pakistani tribesmen.[82]

The ruler of Kashmir at the time asked India for help in repelling the tribesmen, but India demanded that Pakistan should accede to India first. Kashmir agreed and India sent forces to Kashmir to block the invasion. At this point India divided Kashmir into Pakistani and Indian controlled areas. This partition continues to date with the dividing line known as the Line of Control.[83]

The refusal of Pakistan to accept the accession to India of Jammu and Kashmir resulted in the first of three wars between Pakistan and India. This division created a majority Muslim area in the West and East, resulting in three major ethnic areas: 1) Ladakh (Buddhist); 2) Vale of Kashmir (controlled by India), and 3) the part now controlled by Pakistan who are majority Muslim. Sheikh Mohammad Abdullah, the leader of the largest Muslim political party in the state - the National Conference - ratified the accession into India. This was the true beginning of the Jammu and Kashmir conflict and the ongoing dispute of land ownership. Kashmir is located in the northwestern part of the Indo-Pakistani subcontinent, and borders Pakistan, Afghanistan,

---

[82] Library of Congress – Federal Research Division; Country Profile: India December 2004
[83] US State Department Report, *The truth on Kashmir and Terrorism in India*.

China, and India illustrated in Figure 3:

Conflict Region of Jammu and Kashmir

Figure 3 Map of Jammu and Kashmir [84]

The region is roughly 86,000 square miles with an estimated population of 13 million people. The state of Jammu and Kashmir's landmass is larger than 87 independent countries, with its population greater than 114 countries. The present cease-fire line, recognized by the international community, divides the state into two parts, giving 63 percent of the area to India, including the Srinagar Valley, Jammu and Ladakh. The remaining 37 percent belongs to Pakistan, to include the Azad Kashmir.[85] This historical overview of India's origins allows the reader to understand the causes of the Jammu and Kashmir conflict before a country assessment and COIN plan was developed.

---

[84] Map of South Asia from University Texas. Accessed on 1/26/2006 at http://www.lib.utexas.edu/refsites/statistics.html

[85] BRIG Syed Shakeel Hussain, *Jammu and Kashmir*: (U.S. Army War College, Student, 2002).

This section described the history of India and the demographics of Kashmir. To end the 59-year conflict over the partition, India and Pakistan are currently considering negotiations regarding Jammu and Kashmir. The next section will continue the examination of India, but will focus on the political, religious, military, economic, and social conditions that contributed to their COIN operation's success. In addition, this examination will identify the ideal information sources and decision-makers within their institutions. Discussions of the Indian IW capabilities, which are similar to the U.S. IO capabilities, are the topics in this section as well.

Conditions in India's Operating Environment

This section will examine the political, religious, military, economic, and social institutional makeup of the Indian government. The institutions mentioned collect and analyze information and inform the decision-maker in formulating a COIN plan. The primary decision-maker in the Indian government is the Prime Minister. Influential to the Prime Minister's decision-making are state and local elected officials, the adversaries' actions, and more importantly his Council of Ministers. Within this body the Prime Minister collaborates, synthesizes, and articulates his vision and intent.

Political: India is a democratic republic with a central government and is legally established based on the amended 1950 constitution. The constitutional basis for the central government is much like the British parliamentary system with the separation of powers occurring within the executive, legislative, and judicial branches. The central government exerts greater control over the union territories than over the states. Each state has a governor, legislature, and council of ministers headed by the chief minister who acts on behalf of the prime minister. Both governors and ministries serve as decision-makers within their respective districts.[86] The Indian parliament is composed of a lower house (the Lok Sabha) and an upper house (the Rajya Sabha). These

---

[86] Ibid, 32.

parties are agents within the information environment. Members of parliament and state

legislative assemblies elect India's prime minister and president. Over time, the prime ministry,

along with the Council of Ministers, has become the centralized source of power making the

presidential capacity more of a ceremonial position than one of authority. The political climate

within India remains challenged at several layers, mainly by a large number and growing

diversity of political interest groups (agents in the information environment). These political

interest groups split mainly among ideologies. Some amalgamation of the various social groups

have held elected office, including women, Sikhs, Muslims and Daltis who served as either

president or prime minister. This demonstrates the capacity of the political institution to extend

political awareness to new social groups, which causes political development.

The Indian National Congress (INC) was the dominant political party from the partition until

their defeat in December 1977. The INC regained political dominance from 1989 to 1998, but

lost in 1998. The dominant political ideology then was often associated with the Bharatiya Janata

Party (BJP), which was in power from 1998 to 2004 and led by Prime Minister Atal Bihari

Vajpayee. The BJP party was defeated in 2004 when the INC candidate Manmohan Singh

became Prime Minister. This party is often associated with Hindu nationalism, which is facing

difficulty in its political capacity to address the numerous problems of poverty, substantial

income gaps between the wealthy and poor, and numerous insurgencies that threaten the

territorial integrity.

Using the author's definition of information, India's Prime Minister is its decision-maker.[87]

The Prime Minister exerts his power through the collaborative environment of the military and

the Council of Ministers. The Council of Ministers and the military serve as ideal information

sources and influencers of information within India. This is evident because the Prime Minister

---

[87] Ministry of Defense, *Government of India*. Available at
http://www.mod.nic.in/aforces/body.htm. accessed 1 November 2005.

and Council of Ministers create the national security policy. Underneath the Prime Minister and Council of Ministers is the civilian bureaucracy, which exercises influence through the Defense Minister's Committee of the cabinet, supported by the Chief of Staff's Committee. India's foreign relations with all major nations traditionally comprised of the principles of nonalignment and the pursuit of India's own economic development. A post-Cold War shift in military power and concerns with terrorism have led India to create stronger bilateral relations with China, Israel, the United States and other nations. This played a critical role in India's perception management campaign as the rising regional power in South Asia.

As will be seen, India primarily uses civil authorities augmented by paramilitary forces to conduct counterinsurgency operations.

Religion: The Hindu and Muslim people of Kashmir have lived relatively peacefully since the 13th century when Islam became the majority religion in Kashmir. Throughout history, certain Kashmiri Muslim leaders have had a narrow view of history and subjected the Hindu minority people to cruelty. The current armed secessionist movement in Kashmir mostly derives its inspiration from these people. During the conflict, some 20,000 Hindus were killed and over 500,000 have become refugees due to the violence in Kashmir. Approximately 80.5 percent of India's population is Hindu, 13.4 percent is Muslim, 2.3 percent is Christian, 1.9 percent is Sikh, 0.8 percent is Buddhist and 0.4 percent is Jain. Another 0.6 percent belongs to other faiths such as Zoroastrianism and numerous religions associated with Scheduled Tribes.[88] The Indian controlled Jammu and Kashmir state religious make-up is as follows: 65 percent Muslim, 33 percent Hindu, and 3 percent Buddhist. In the Kashmir Valley region, it is 98 percent Muslim, with all other religions accounting for 2 percent of the population.[89] The vast religious participants in the contested area of Jammu and Kashmir represent ideal information sources.

---

[88] Ibid, p 8.
[89] Ibid, p 8-10.

The populace in these areas can be proponents or opponents to the Indian effort to defeat the insurgents. India's goal in this area is one of continuing to promote individual religious beliefs without violating human rights.

Military and Civil Authorities: The continual presence of terrorists and fundamentalists has forced India to maintain a robust military and civil defense force for those threats. India's National Army's (INA) security objectives have revolved around its core values of democracy, secularism, and peaceful co-existence, along with its social and economic development. The president is the supreme commander of the armed forces and acts in accordance with the recommendations from the Cabinet of Ministries and Prime Minister. The key military roles for India as outlined in their national strategy are:

1. Defending the country's borders as enshrined in the Constitution.
2. Protecting the lives and property of its citizens against war, terrorism, nuclear threats, and militant activities.
3. Protecting the country from religious instability and other forms of radicalism to include extremism emanating from neighboring states.
4. Securing the country against the use or the threat of use of weapons of mass destruction.[90]

The Indian civil-enforcement is a robust agency with powers similar to the military. The civil defenses, along with the paramilitary, are the major defense forces combating the insurgents. The civil authorities have established a large presence in India by setting up police precincts. These increased numbers of police precincts created the first visible signs of decreased terrorist activities. Although the national military forces combat the terrorists as well, they primarily focus on enforcing the national security strategy by protecting the country's borders. The major threat to Indian national security is China. This perceived Chinese threat comes from numerous

---

[90] Ministry of Defense, *Government of India,*.

attempts by China to isolate India militarily and diplomatically from the rest of the world.[91] With a regionally focused national security challenge, India's greatest challenges are internal threats, categorized by religiously oriented conflict or ethnic violence with separatist objectives.

India relies on 17 federal paramilitary and police organizations for border and internal security. Although the paramilitary is equipped similarly to the Indian Army, its mission is one of support. The paramilitary task and purpose has migrated to one of COIN throughout the years due to the increase of insurgent activity across the state. Approximately 400,000 Indian military and paramilitary forces serve in Kashmir along the Line of Control (LOC). This large force patrols both Pakistani and Chinese LOC in an effort to deter insurgent cross-border infiltration into Kashmir.[92]

In summary, India's national security strategy and threat assessment allows their military the ability to safeguard India's security interests that extend from the Persian Gulf in the west to the Straits of Malacca in the east, and from the Central Asian Republics in the north to near the equator in the south. India's local law enforcement, assisted by the military largely battling the insurgents, gives the impression that the threat is under control locally and is not a state problem.

Economics: Although two-thirds of India's workforce is in agriculture, services are the major source of economic growth. India's population is largely rural, with 74 percent residing in 600,000 villages. Of India's total 3.3 million square kilometers of land, about 55 percent is available for cultivation. The remainder is dense forest, desert, or fallow land. Of that 55 percent, only 33 percent has irrigation available. These geographic limitations contributed to how India developed its counterinsurgency plan. Some regions within Jammu and Kashmir are not under the influence of the Indian law-enforcement or paramilitary forces.

---

[91] Library of Congress – Federal Research Division; *Country Profile: India* (December 2004).
[92] NGIC. *How They Fight: Armies of the World (NGIC-1122-0205-99, 1998).* Available at http://www.ngic.army.smil.mil/products/htf/NGIC-1122-0205-99/SC8.htm. accessed on 1/31/2006.

India's 2004 GDP estimate was $3.319 trillion, with 2.93 percent or 18.86 billion in expenditures going to the military.[93] Military spending has increased by 28 percent since 2001. In 1991, the government took steps to cease restrictive government interference and reform the economy after a severe foreign exchange crisis. The reforms were in the areas of foreign investment and exchange regimes, and a reduction in tariffs and trade barriers. These initiatives resulted in higher growth rates, lower inflation and increased foreign investment in the Indian economy. All of these measures were part of India's process of becoming the South Asian regional hegemon. The economic growth in Kashmir is showing growth due to the Indian government's investments in health care, education, infrastructure, and utilities.

Social: A 2005 CIA report estimated India as having the world's second largest population at 1.1 billion. It has a population growth rate of 1.4 percent and a life expectancy at birth of 64 years of age. These figures include the second largest Muslim population in the world, with 180 million Muslims living in India and 140 million living in Pakistan. In 1947, 40 percent of Pakistan was non-Muslim but today it is only 3 percent non-Muslim: 25 percent of India was then Muslim, but only 18 percent of Indians are Muslim today.[94] These figures indicate the Muslim population is reaching pre-partition demographics in India and that the possibility of ethnic cleansing within Kashmir is occurring.

The vast majority of Kashmiris oppose India and Pakistan going to war to find a permanent solution to their situation. The majority believe the correct way to bring peace to the region is through democratic elections, ending violence and economic development.[95] Results from a MORI April 2002 poll stated that the consensus across the region was that it is not possible to hold democratic elections while violence continues – with 65 percent in agreement and 34 percent

[93] *India available* at http://www.cia.gov/cia/publications/factbook/geos/in.htm accessed on 2 January 2006.

[94] CIA Fact book *India"*

[95] Available at www.MORI.com. *Kashmiris Reject War in Favor of Democratic Means* accessed 3 February 2006.

in disagreement.[96] Because India's economy is mainly agrarian, many youth are unemployed consistently throughout the year and easily recruited into the insurgent groups operating within the region.

Information (India's Information Warfare Capabilities)

India is acquiring the capability and the capacity to influence political and economic developments within South Asia. Although information is not a dominant military or economic power, information has the capacity to increase those particular areas. A recent Department of State Strategic Communications Fact Sheet, dated February 27, 2006, stated, "The U.S. views India as a rising global power and partner, one whose interests converge in important respects with those of the United States. The U.S. also anticipates that India will play an increasingly important leadership role in Asia in the 21st century."[97] This statement alone sends a bold message indirectly to Pakistan and other regional states that the U.S. is concerned about the future of India and will provide assistance through military-to-military relations and promoting democracy. It also is a form of Public Diplomacy in support of India.[98]

The IO activities of physical destruction, PSYOP, public diplomacy and civil-military operations have supported the COIN operations in Kashmir, but the greatest weapons against India's insurgent activity have come through the use of civil-military forces and military support to public diplomacy. While these capabilities are not yet fully developed, the open source doctrine of the U.S. has allowed India to conduct detailed analyses on the activities associated with information operations. India PSYOPs focus is domestically using the internal state press and media. The past relationships with the Indian medias ability to report fairly and accurately about the military have placed military leaders on the defensive causing them to deny the media

---

[96] Ibid. Kashmir Rejects War.
[97] U.S. Department of State "The United States and India: A Growing Strategic Partnership" accessed at http://www.state.gov/r/pa/scp/2006/62209.htm on February 27, 2006.
[98] Ibid.

true access on sensitive subjects.[99] The INA has its own propaganda-generating web site to counter the pro-Muslim Kashmir sites. This site allows the Indian military to articulate its message unhindered about insurgents to both Hindu and Muslim populations. The shortfall of this open source site is that it has allowed several hacker attempts to enter into the Indian defense information infrastructure.[100] The INA civil-military operations include outreach programs in Kashmir. The military has assisted in renovating several schools and provided school supplies to children. These gestures have increased the trust of the Indian security forces in the area and may possibly deny the terrorist a sanctuary.[101]

In summary, the claims India is using to tie their COIN with the GWOT by categorizing the conflict in Jammu and Kashmir as an insurgency supported by Pakistani terrorists, will deny the political credibility of any organization within the region of Jammu and Kashmir. The challenge India's government faces are how to incorporate a Muslim state into a majority Hindu society that will allow fair representation of its participants. India has struggled with this issue since the onset of violence in Jammu and Kashmir.

After a description of major terrorist organizations operating within Jammu and Kashmir and the role these organizations play in India's information environment, the next two sections will continue the discussion of Indian IW capabilities of civil-military and public diplomacy.

India's Counterinsurgency Threats

This section examines the counterinsurgent groups operating within India. The insurgents' goals and their political and military performance will determine the conditions under which

---

[99] Available at www.hinduonnet.com/thehindu/thescript/fline/htm.
[100] BBC Online Network *"War on Words" Available* at http://news.bbc.co.uk/1/hi/world/monitoring/200708.stm accessed 4/6/2006.
[101] *Indian Army Renovates 66 schools in Kashmir*. Available at http://www.india-defence.com/reports/1346, accessed on 2/4/2006.

India employs resources in its COIN operations. This categorization will facilitate understanding of how India's IW capabilities support its COIN operations.

Although India has more than 30 known insurgent groups currently operating within Pakistan and India, this section focuses on the three dominant groups affiliated with the Jammu and Kashmir conflict; the Pakistani Islamic extremists Harakat ul-Mujahidin (HUM); Movement of Holy Warriors, Lashkar-e-Tayyiba (LT) Army of the Righteous; and the Lashkar I Jhangvi (LJ) Army of Jhangvi.[102] A brief sketch of their objectives, funding, and political position will identify the key capabilities India planned to attack during their COIN operations. The Indian government has designated these insurgent groups' terrorist organizations, which is a key point in establishing a strategic message to the international community.[103]

The first insurgent group in India's COIN operations is Harakat ul-Mujahidin (HUM) Movement of Holy Warriors. HUM is a Pakistani-based Islamic militant group that operates as an insurgent/terrorist group in the Indian occupied portion of the Jammu and Kashmir. The HUM declared goal is the liberation of Jammu and Kashmir through jihad. The group has a Sunni Islamic separatism ideological base. HUM veterans grew out of the Afghan war and initially founded the Harakat ul-Ansur (HUA) in 1993 with the same goal of liberating Jammu and Kashmir from India. The HUA renamed itself Harakat ul-Mujahadin (HUM) after the United States declared the group a foreign terrorist organization in 1997. This group receives its funding from various donations, such as Saudi Arabia, and other Islamic states such as Pakistan and Kashmiris. Although they do not pose a direct threat to the U.S. government their leader, Fazlur Rehman Khalil, had alleged links to Osama Bin Ladin and had signed his fatwa in 1998 calling for attacks on U.S. and Western interests. In 2003, HUM began using the name Jamiat ul-Ansar (JUA).

---

[102] U.S. Department of State, *Patterns of Global Terrorism* 2002, April 30, 2003.
[103] Indian Ministry of Home Affairs. T*he Prevention of Terrorism Act 2002* Available at http://mha.nic.in/poto-02.htm#schedule.

The ideology of Lashkar was originally Wahhabi, but it gradually distanced itself from Saudi Arabia based on the lack of no true Islamic world had not been established. The two groups operating within Kashmir all share the same tie: to oppose any concession in Kashmir and see its aim in the liberation of all Muslims in India and eventually the establishment of Islamic rule across the world "global caliphate." [104]

The Lashkar-e-Tayyiba (LT) Army of the Righteous, Lashkar-e-Tobia, al-Monsooreen, Army of the Pure and Righteous; is the armed wing of the Pakistan anti- U.S. Sunni religious group. It is one of the best-trained fighting groups in Kashmir against India. Although no evident connection to a political party exists, it has conducted multiple attacks on Indian troops and civilian targets in Jammu and Kashmir. The recent capture of a senior al-Maida in an LT safe house suggests some linkage between them and the movement of al-Maida inn Pakistan.[105]

The last known and reported insurgent group operating within Kashmir is Lashkar I Jhangvi (LeJ) Army of Jhangvi. This group is the militant offshoot of the Sunni sectarian group Sipah-i-Sahaba Pakistan (SSP). The group's aim is to reform Pakistan into a Sunni state, primarily through violent means. This group has claimed responsibility for killing American oil workers in 1997 and the assassination attempt of the Pakistan Prime minister Nawaz Sharif in 1999. The group is also responsible for taking part in the kidnapping and murder of the U.S. journalist Daniel Pearl.[106] India has included this group on its known terrorist exclusion list, but the U.S. has not added them to its list as of February 2006.

---

[104] Walter Laqueur, *No End To War: Terrorism in the 21st Century*. (New York and London: Continuum International Publishing Group, 2004),
[105] DOS Designated Foreign Terrorist Organization
[106] National Memorial Institute for the Prevention of Terrorism *India.* Available at http://www.The Terrorism Knowledge Base.com. accessed 4February 2006.

Although the insurgents are poorly equipped, they have alleged connections with Pakistani Islamic organizations and receive funding from al-Qaeda.[107] Additionally, India suspects that the insurgents operating within Jammu and Kashmir are receiving training in the Taliban-ruled Afghanistan. The insurgents' goal is the complete union of all Muslims in the region surrounding Pakistan and the restoration of Islamic law over the state of India.[108] With India's stance on secularism, this view serves as a flashpoint in the multi-ethnic state where the detonation of nuclear weapons is a major concern. Diplomatic resolve seems to be the only solution in ending this conflict, with international involvement of both India and Pakistan who have stated future "talks" may lead to a settlement over the Jammu and Kashmir conflict.[109] The next section will discuss how India conducted COIN operations through the employment of local law enforcement and paramilitary forces in Jammu and Kashmir.

ANALYSIS OF INDIA'S COIN

This section will examine three factors of the Indian government's response to the insurgency in Jammu and Kashmir. The examination will identify India's IW capabilities that are similar to those of the U.S. IO activities utilized in COIN operations. In applying this framework, India used three factors to establish a COIN plan that is consistent with existing fundamentals of COIN operations; correct analysis of the threat, use of public diplomacy, and the employment of paramilitary forces.[110] The methods India used played a vital role in the state's ability to limit the insurgents' operational reach; however, the state response has not significantly decreased the influx of foreign terrorists entering the country. Although, there is no public document detailing

---

[107] Markle Foundation. *Terrorism: Q & A "Kashmir Militant Extremists". Available at http://cfrterrorism.org/groups/harakat_print.html. accessed 9/23/2005.*
[108] SATP *Lashkar-e-Tobia (LT)*available at http://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba.htm. accessed 2/7/2006.
[109] BBC *Kashmir Dispute: Q&A*. Available at http://news.bbc.co.uk/1/hi/world/south_asia/2739993.stm. accessed 3/7/2006.
[110] For the purpose of this research, the terms and figures associated with paramilitary forces include the civil-law enforcement personnel also.

the elements of its COIN plan, it is clear that civil-military operations, public diplomacy, PSYOP and physical destruction activities were the key IO capabilities that supported the four factors India used in denying the insurgents Jammu and Kashmir.

India's information environment included global perceptions of the Jammu and Kashmir conflict and the linkage between terrorism and Pakistan, religious beliefs and value systems, past differences and conflict. Other elements populate the information environment that affected development of India's COIN plan; for example, the position of the international community and the U.N. Security Council and humanitarian relief agencies have all influenced India to utilize paramilitary and border security forces to conduct COIN.[111] The concern of the international community for stability within the South Asian region influenced the Prime Minister of India – the decision maker – in designing India's COIN plan. The ideal information source that informed the Prime Minister was the Council of Ministers, paramilitary and border security forces. The Council of Ministers' power comes from interaction with the Indian National Army (INA). Although the Prime Minister has the final approval for India's national security strategy, the Ministers and INA serve as the Prime Minister's collaborative information environment through the continual sharing of information.

India's two strategic goals for its COIN campaign are creating a democratic government friendly to regional and western interests, and the removal of the conditions that create insurgent safe havens. These objectives are consistent with their national security strategy of defending the country's borders; protecting the lives of its citizens against war, terrorism, and militant activities; and protecting the country from instability associated with religious or other forms of radical extremism.[112] With these objectives in mind, India utilized various tactics to combat the

---

[111] Michael Krepon, "A confluence of international and domestic pressure may finally be pushing Indian and Pakistan towards a compromise. (23 December 2004) Available at http://www.pugwash.org/reports/rc/sa/SAS2004-media-krepon.htm accessed on 2/4/2006

[112] Ministry of Defense, *Government of India.*

insurgent threat in Jammu and Kashmir in an effort to decrease hostilities between "citizens" and to restore stability within the region. India's ability to identify the insurgents allowed the government to understand the motivation and social dynamics of the populace in the affected area. India's analysis led to speculations that a large number of foreign fighters, mainly from Pakistan, were entering their country. This analysis came from the change in terrorist tactics, where the number of attacks decreased but the number of deaths increased. The large number of deaths was due to the insurgents' increased sophistication in conducting coordinated attacks. The security forces saw a move from kidnapping to bombing attacks and the use of remote controlled devices to detonate explosives. The ideal information source for this analysis comes from the media, local population, captured insurgents, and ongoing battlefield assessments. India's analysis created a shift in tactics that led to the construction of a 750km fence along the LOC.[113] The fence served as a physical and psychological deterrent to terrorist infiltration from Pakistan, Afghanistan, and China, and to the insurgents currently operating within India. Additionally the fence created a perception in the international community that India will not support terrorist training nor allow insurgent activities within its borders.

Although the extremely fragmented terrorists groups operating within India are not directly attacking the U.S., their motives and ideologies are consistent with the acts of global terrorists, which are of interest to the U.S.G. These insurgents practice protracted warfare and seek to replace the existing secular state government with one of total Islamic control. Even though the insurgents in Kashmir are fragmented, their common goal - a complete Islamic state - allows them to achieve tactical objectives indirectly through localized attacks, but also creates operational challenges when trying to unite the state of Jammu and Kashmir under total Islamic law. The increasing number of Al Qaeda tactics and foreign fighters indicates the evidence of insurgent groups with similar interests working with one another.

---

[113] Biswas, Soutik, "Indian Army Wary of Open Border". *BBC News World South Asia.* Available at http://news.bbc.co.uk/1/hi/world/south_asia/4359914.stm. Accessed 11/1/2005.

India's public diplomacy and IW related activity of military support to public diplomacy are two-fold. India wants to continue its advancement as a secular government with fair government representation and portray Pakistan as being a state supporter of terrorists and a state who allows insurgent infiltration into the Jammu and Kashmir region. The large Muslim population living under a constitutional and secular political arrangement directly challenges Pakistan's national identity.[114] The IO activity of the military support to public diplomacy in the Jammu and Kashmir conflict is limited, but focuses on an effort to continue the suppression of the insurgency and redefine the Indo-Kashmiri relationship. The public message should reorient the populace of the notion that the Jammu and Kashmiri dispute is over geography, but suggests the larger issue that it is part of the Islamic Jihad waged by Islamic fundamentalists operating from countries like Pakistan, Saudi Arabia, and Taliban occupied Afghanistan.[115]

One of India's central strategic problems is how to achieve unity of the subcontinent and protect it from outside powers. India's purchasing power, military, and open society of governance will allow it to continue to advance at a rate far above its regional competitors in South Asia. India chose to combine domestic and international policy along with civil authorities as an option of perception management. This was an attempt to create diplomatic and political support in the international community and an attempt by India to begin labeling the insurgents as part of the global terrorist structure supported by Pakistan. India has continued to push this propaganda and deception overtly through a technique similar to the U.S. information operations, known as information warfare (IW). The concept of information warfare in India dates back to its partition and the claims it made to the United Nations in 1948 over the dispute in Jammu and Kashmir. Additionally, the unsubstantiated claim of Pakistani to be supporters of the insurgents continues to shape the public perception concerning Pakistan and Indian relations.

---

[114] J.N. Dixit, *India-Pakistan in War & Peace.* (New York: Routledge, 2004), 391.
[115] Alexander, *Combating Terrorism. 336.*

The lesson for the operational level IO planner conducting COIN in South or Central Asian countries is to focus public diplomacy on a comprehensive security strategy that addresses domestic and international issues, such as internal security, repatriation, and restoration of human rights. The availability of a coherent definition of information allows the planners to collect and analyze information within systems that contribute to the current tension in Kashmir. The strategy here is to continue to allow India to work with the international community, as it has signed numerous bilateral agreements against terrorism, which may ultimately lead to a consensus about terrorism within the United Nations.[116] This policy does not give up hope of improved relations with neighboring countries, but allows India to continue the fight on terrorism and support of the GWOT.

The final tactic India employed was the use of paramilitary forces to augment border security and military forces. The capabilities these forces employ enable the functionality of CMO and physical destruction IW concepts. India's main response to the insurgency has been consistent with its internal mechanism of state security. India considers its insurgency problem in Jammu and Kashmir as an unresolved issue of law and order within the state. This concept allows their local civil authorities to enforce national regulations concerning terrorism. This process enhances the judicial and extrajudicial punishment at the local and state levels. The utility of the Indian employment of civil law enforcement is consistent in how a state imposes the rule of law in settling complaints through the judicial system. Since India's paramilitary forces began assisting the military and border security, the number of terrorist attacks has decreased but the number of deaths associated with terrorism has remained considerably high.[117] The Indian government sees the paramilitary force augmenting the local police as a success in reducing terrorism. The Indian government divided Jammu and Kashmir into fourteen police districts known as "revenue

---

[116] India seems more willing to work with the international community to control terrorism. Alexander, *Combating Terrorism.* 333.
[117] Alexander, 312.

districts." This division doubles the work force required to provide security in the remote regions of Kashmir, which leaves some areas unsecured and patrolled. The challenge is that the ratio of paramilitary and local police to population in Kashmir makes any possibility of a safe and secure environment impossible. Although the security force to population ratio was low, their initial pattern analysis that the population settlement was dispersed over the Kashmir region was mitigated by executing a layered approach of interlocking police districts to reinforce existing civil law enforcement structures.[118] The deployed force's goal was to dominate the entire area "grid." Another tactic was the fencing of the LOC. As stated earlier, this created a psychological effect on the insurgents as the interlocking paramilitary and security forces patrolled the grid. In theory, the insurgents would move toward the heavily defended fenced LOC, thus sealing off the battlefield in favor of the Indian forces. This theory continues to work, but is hinged on the relationship the police and paramilitary have with the local population. This is critical in the success of their COIN operations, as the remote regions of Kashmir are not all patrolled by Indian forces. The insurgents do not heavily occupy those areas that favor police action against terrorists, but in the areas where police and military patrols are minimal. The insurgents in the Jammu and Kashmir region have the highest insurgent activity where grievances against the Indian government and security forces occur.

In summary, India achieved its tactical objectives and local security forces have prevented the insurgents from overrunning cities, but the strategic and operational objectives have fallen short of their national security goals. India considers the operational challenge of the insurgency as one of law and order, which refers to enforcing the normal mechanisms of the political system of the state. India has created a host of state policies that ensure the future of its current political culture. Some of these policies include the Terrorist and Disruptive Activities (Prevention) Act

---

[118] Ibid.

1987, or TADA, and the Prevention of Terrorism Ordinance, 2001, or the POTO that later became the Act of 2002 (POTA).[119]

Since 2001, more than 32 groups were included on the Indian Government's list of terrorist organizations and an undisclosed number of groups declared unlawful. Other policy measures include India's involvement with the US-India Counterterrorism Joint Working Group founded in 1999. The working group agreed to pursue closer cooperation on shared counterterrorism goals. The parliament has enacted an anti-money laundering law that provides the legal basis for establishing a financial intelligence unit to monitor suspect transactions.[120] It would be an error to trivialize the ongoing conflict in Jammu and Kashmir as a territorial one; instead, it represents one where a secular state seeks to include multi-ethnic and religious groups under one form of government. Strategic communication from both countries should promote Jammu and Kashmir as a state with a valuable past within India a secular state.

A diplomatic breakthrough remains a possibility, if a remote one. Particularly after the 2005 natural disasters, Pakistan and India have increased talks concerning terrorism and the conflict in Kashmir. Although violence in the Jammu and Kashmir continues, key moderate groups among the threats have met face-to-face with India's Prime Minister. Without the combination of public diplomacy and civil-military operations, progress may not have been possible for the security forces efforts to secure the Line of Control.

SUMMARY OF FINDINGS

Currently, India's information warfare capabilities resemble the U.S. information operations core and supporting elements: civil-military operations (CMO), psychological operations (PSYOPS), public diplomacy, and physical destruction. This monograph's premise was that

---

[119] TADA The Terrorist and Disruptive Activities (Prevention) Act (TADA) of 1987 established in camera courts and authorized detention of persons in a "disturbed area" based on mere suspicion. The POTA of 2001 gives the Indian police immense powers of arrest and detention.
[120] Alexander, 312-317.

current U.S. Army Doctrine for information operations was void of a coherent meaning and understanding of the term information. The definition of information provided by the FM and JP 3-13 publication are similar to those mentioned in this monograph, but differs in the packaging of transmissions and the form of information types. The information systems design definition of information was the link between the tangible and intangible elements of information. Planners should consider how the commander conducts information operations in a COIN environment and how the commander assigns value to information from the ideal information sources. Information sources and information operations are subject to change as technology expands into the cognitive and cyberspace dimensions. The ability of commanders and staffs to interpret and assign value to information within the environment will continue to be a challenge for future operations.

Clearly, if the DOD is going to capitalize on the activities of Information Operations, it is necessary to define information and the importance of the commander's ability in accurately assigning value to the elements of intangible collected data. The future battlefield will continue to have organized and disorganized signals of information; the challenge for planners is to synchronize the best available information based on the commander's intent and desired end state. The critical piece for commanders in processing information is for their staffs to provide the decision maker enough data points linked through the physical, informational, and cognitive dimensions. This allows the commander to interpret, assign value to, and prioritize pertinent information.

Indian military thinking developed differently than that of the U.S. for obvious reasons; internal and external threats, social dimensions, and geography has led India to focus its resources on CMO, CNO and PSYOPS. Regional and domestic threats require India to exercise aggressive tactics on combating terrorists and maintaining its borders and international image. The regional threats of China and Pakistan are computer literate and have the propensity to exert force through

computer-networked attacks as demonstrated by Pakistan in late 2003. India has shown that it is capable of deterring internal and external aggression within its borders and will continue to position itself to be the regional hegemony.

Information operations is a process that incorporates the elements of all military activities, which warrants designing operations that integrate effects from friendly physical, cognitive and information capabilities. In order for this to occur, the military commander and staff should acknowledge that every activity the U.S.G. conducts produces information that should be interpreted, analyzed, and incorporated into a coordinated plan of action. The synchronized support of the military information operation activities of public diplomacy and public affairs, in concert with other U.S.G. instruments of national power, assist in advancing the U.S.G. themes and messages. These themes and messages advance U.S. interests and foreign policy throughout the world.[121] Based on the previous understanding that energy produces information, it should be clear that some intended effects would produce results only in the information and cognitive dimensions. These activities mainly result from actions in the PSYOP, PA and public diplomacy systems. India has recognized the importance of perception management and has related perception management to United States' information operations, and uses it in both positive and negative ways to highlight its conflict over Jammu and Kashmir. The IO activity most desirable in resolving the Jammu and Kashmir conflict is public diplomacy; however, both India and Pakistan must allow some concessions for religious indifferences.

BIBLIOGRAPHY

US GOVERNMENT PUBLICATIONS

Bush, George W. The National Security Strategy of the United States of America. Washington, D.C.: The White House, September 2002.

---

[121] Participant Guide, handout from SOUTHCOM (March 2006), E-2.

Bush, George W. National Strategy for Combating Terrorism. Washington, D.C.: The White House, February 2003.

Joint Chiefs of Staff. Joint Publication (JP) 1-02: Joint Doctrine for DOD Dictionary of Military and Associated Terms. Washington, D.C: GPO, 12 April 2001.

Joint Chiefs of Staff. Joint Publication (JP) 3-13: Joint Doctrine for Information Operations. Washington, D.C: GPO, 9 October 1998.

Joint Chiefs of Staff. Joint Publication (JP) 3-13: Joint Doctrine for Information Operations. Washington, D.C: GPO, Revision, Final Coordination 5 July 2005.

Joint Chiefs of Staff. Joint Publication (JP) 3-13: Joint Doctrine for Information Operations. Washington, D.C: GPO, 13 February 2006.

Joint Vision 2020, Chairman of the Joint Chiefs of Staff, Director for Strategic Plans and Policy. Washington, D.C.: U.S. Government Printing Office, June 2000.

Mendhurst, Paul. Global Terrorism: United Nations institute for Training and Research Programme of Correspondence Instruction, 2002.

The World Fact Book http://www.cia.gov/cia/publications/factbook/geos/in.html

U.S. Department of Defense, IO Policy. *Information Operations Roadmap*. Washington, D.C: GPO, October 2003.

U.S Department of State, FY 2003 Performance and Accountability Report accessed on 28 December 2005. http://www.state.gov/s/d/rm/rls/perfrpt/2003/html/28981.html

BOOKS

Bhatt, Shakti. *State terrorism vs. Jihad in Kashmir*. Journal of Contemporary Asia. Manila 2003 Vol. 33, Iss.2; pg 215.

Abuza, Zachary. *Militant Islam in Southeast Asia: Crucible of Terror*. Baltimore: Johns Hopkins University Press, 1981.

Alberts, David; Garstka, John, and Frederick Stein. *Network-Centric Warfare: Developing and Leveraging Information Superiority*. Second Revised Edition. Washington, D.C.: National Defense University Press, 2000.

Alberts, David; Garstka, John; Hays, Richard; and David Signori. *Understanding Information Age Warfare*. Washington, D.C.: National Defense University Press, 2001.

Alexander, J.B. *Future War: Non-Lethal Weapons in the Twenty-First Century Warfare*. New York: St. Martin Press, 1999.

Alexander, Yonah. *Combating Terrorism: Strategies of Ten Countries*. Ann Arbor, Michigan: The University of Michigan Press, 2002.

Arquilla, John. *Conflict in the Information Age*. Monterey, CA: Naval Postgraduate School, 2001.

Arquilla, John and Ronfeldt, D. Dr. In *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA.: Rand Corporation, 1997.

Celeski, Joseph. Operationalizing COIN. JSOU Report 05-2 (Hurlbert, Florida: The JSOU Press, 2005)

Cohen, Stephen P. *India Emerging Power*. Washington, D.C: Brookings Institution Press, 2001.

Denning, Dorothy. *Information Warfare and Security*. Addison Wesley Longman, Inc., 1998.

Dixit, J.N. *India-Pakistan in War & Peace*. New York: Routledge, 2004.

Esposito, John L. The Islamic Threat, Myth or Reality. Third Edition. New York. Oxford University Press, 1999

Fair, Christine C. *Urban Battle Fields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan*. Santa Monica, CA.: RAND Corporation, 2004.

Hoffer, Eric. *The True Believer: The Thoughts on The Nature of Mass Movements*. New York. Harper Collins Publishers, 1951.

Hoveyda, Fereydon. *The Broken Crescent: the Threat of Militant Islamic Fundamentalism* Westport, Conn.: Praeger, 1998.

Landman, Todd. *Issues and Methods in Comparative Politics: An Introduction*. Second Edition. London and New York.: Routledge Taylor & Francis Group, 2003.

Laqueur, Walter. *No End To War: Terrorism in the 21st Century*. New York and London.: Continuum International Publishing Group, 2004.

Leather, Kaia. *Kashmiri Separatists: Orgins, Competing Ideologies and Prospects for Resolution of the Conflict*. New York: Novinka Books, 2003

Khalilzad, Zalmay and John White. *The Strategic Appraisal: The Changing Role of Information Warfare*. Santa Monica, CA.: Rand Corporation, 1999.

Moore, Barrington. Jr. *Social Origins of Dictatorship and Democracy*. Boston, Beacon Press, 1966.

Majumdar, B.N. *A Short History of the Indian Army*. New Delhi, 1967.

National Ground Intelligence Center. *India: Assessment of Adversary Information Operations Capabilities*.

Nye, Joseph S. Jr. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2005.

Oldenburg, Philip. *India Briefing, 1993*. San Francisco, CA.: Westview Press, 1993.

O'Neill, Bard E. *Insurgency and Terrorism: Inside Modern Revolutionary Warfare. United States of America*.: Brassey's Inc., 1990.

Ottaway, Marina. *Democracy Challenged, The Rise of Semi-Authoritarianism*. Washington, D.C.: The Brookings Institute Press, 2003.

Rowe, Greg. *Applying the Principle of War to Information.* (Joint Information Operations Center, IO Sphere Winter 2006 edition)

Schofield, Victoria. *Kashmir in Conflict: India, Pakistan and the Unending War*. London and New York: I.B. Tauris, 2003.

Sun Tzu, *The Art of War*, ed. and trans. Samuel Griffth, New York: Oxford University Press, 1971.

Taylor, Philip M. *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day*. New York and Vienna.: Springer, 1998.

Tibi, Bassam. *The Challenge of Fundamentalism: Political Islam and the New World Disorder*. Berkeley, California: University of California Press, 2002.

Turban, Kate L. A Manual for Writers of Term Papers, Theses, and Dissertations. Sixth ed. Chicago: University of Chicago Press, 1996.

Wilson, Ira G. and Marathann E. Wilson. *Information, Computers, and System Design*. John Wiley and Sons, New York: 1967.

Whitten, Jeffery, Lonnie Bentely and Kevin Dittman. *Systems Analysis and Design Methods*. Sixth Edition. Boston, MA.: McGraw Hill Companies, 2004.

MONOGRAPHS

BRIG Syed Shakeel Hussain. Jammu and Kashmir: U.S. Army War College, Student Monograph, 2002.

Eassa, Charles. *U.S. Armed Forces Information Operations – Is the Doctrine Adequate?* (Fort Leavenworth, Kansas. Student Monograph, 1999), 5Latimer, William S. What can the United States Learn from India to Counter Terrorism?: Naval Postgraduate School, March 2004.

Kuehl, Dan. Dr. Information Operations, Information Warfare and Computer Network Attack: Their Relationship to Nation Security in the Information Age. National Defense University Press, 2003.

Morthland, Samuel P. Information Operations: The Need For A National Strategy: Naval Postgraduate School, Student Monograph, 2002.

REPORTS

ADCSINT THREATS, TRADOC DCSIN; White Paper: Contemporary Operating Environment. February 2, 2000. (Provided by Mr. Walter Williams)

State Sponsors of Terrorism accessed 01/12/2006 at http://www.state.gov/s/ct/c14151.htm

Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science Board Task Force on Strategic Communication.* Washington, D.C. September 2004.

Nasr, Vali. Pakistan: Balancing Reform and Counterterrorism. Washington, D.C.: FDCH Congressional Testimony, 2004.

Ministry of Defence, Government of India. Accessed 11/1/2005 at http://www.mod.nic.in/aforces/body.htm

ARTICLES

Bruce Lawrence, *Messages To The World: The Statements of Osama Bin Laden.* (London: Verso, 2005), 100. Statement from Osama Bin Laden to his "Brothers in Pakistan, September 24, 2001

Grau, Lester. *Kashmir: Flashpoint or Safety Valve*: Military Review, (July-August 1999), accessed on 21October 2005 http://fmso.leavenworth.army.mil/documents/kashmir/kashmir.htm.

Kashmiris Reject War in Favor of Democratic Means accessed 3 February 2006. Available at www.MORI.com.

National Ground Intelligence Center (NGIC). *How They Fight: Armies of the World (NGIC-1122-0205-99, 1998).* Available at http://www.ngic.army.smil.mil/products/htf/NGIC-1122-0205-99/SC8.htm. accessed on 1/31/2006

SOUTHCOM *Participant Guide, Blue Advance Tier I Academics.* March 2006

World Almanac Tool: India Country Facts accessed on 11 January 2006; http://www.aneki.com/students.html

Washington Post: Bush Defends Spying Program "As Necessary" to Protect U.S. accessed on 24 January 2006; http://www.washingtonpost.com/wp-dyn/content/article/2006/01/01/AR2006010100428.html

INTERNET SITES

 Accessed on 20 January 2006 at http://www.osac.gov/Groups/index.cfm

Biswas, Soutik, "Indian Army Wary of Open Border". *BBC News World South Asia.* Available at http://news.bbc.co.uk/1/hi/world/south_asia/4359914.stm. Accessed 11/1/2005

BBC *Kashmir Dispute: Q&A.* Available at http://news.bbc.co.uk/1/hi/world/south_asia/2739993.stm. Accessed 3/7/2006

BBC Online Network *"War on Words" Available* at http://news.bbc.co.uk/1/hi/world/monitoring/200708.stm accessed 4/6/2006.

Markle Foundation. *Terrorism: Q & A "Kashmir Militant Extremists". Available at http://cfrterrorism.org/groups/harakat_print.html. Accessed 9/23/2005*

National Counterterrorism Center. Available at http://www.tkb.org/NCTC/MapModule.jsp accessed on 20 January 2006

South Asia Terrorism Portal (SATP): "Truth about Kashmir" Available at www.satp.org/satporgtp/publication/Faultlines/volume16/Article1.htm. Accessed on 1/31/2006.

SATP *Lashkar-e-Tobia (LT). A*vailable at http://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/lashkar_e_toiba.htm. accessed 2/7/2006

Kashmir http://www.kashmir-information.com/LegalDocs/SecurityCouncil.html

Wikipedia, Information. Accessed on 24 January 2006 at http://en.wikipedia.org/wiki/Information

The Truth about Kashmir accessed on 31 JAN 06 at www,satp.org/satporgtp/publication/Faultlines/volume16/Article1.

International law on terrorism, accessed on 31 JAN 06 at, http://www.ksg.harvard.edu/terrorism/readings/international/international_law.html

APPENDIXES A (Glossary of Terms)

Counterinsurgency: Those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat an insurgency. Also called COIN. (JP 1-02)

Information: 1.) Facts, data, or instructions in any medium or form. 2.) The meaning humans assign to data by means of known conventions used in their representation.

Information Assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and no repudiation. (JP 1-02)

Information Operations: The employment of the core capabilities of electronic warfare, computer network operations,, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversary human and automated decision-making while protecting our own. (JP 3-13)

Information Environment: The aggregate of individuals, organizations, and systems that collect, process, or disseminate information, also included is the information itself.

Insurgent: Member of a political party who rebel against established leadership. (JP 3-07.2)

Military Information Operations: Military information operations are used to some degree in all ranges of military operations, from offensive to the adaptive and emerging stability and support. Current doctrine suggests that military information operations is an enabling operation

Operational Environment: A composite of all conditions, circumstances, and influences, which affect the employment of military forces and bear on the decision of the unit commander.

Perception Management: Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives.

Terrorist: An individual who uses violence, terror, and intimidation to achieve a result. (JP 3-07.2)

Threat: Any specific foreign nation or organization with intentions and military capabilities that suggest it could be adversarial or challenge the security interests of the U.S., its friends or allies. (COE Whitepaper, February 2000) For the purpose of this paper, threat is a plausible, flexible military and non-military force representing a composite of varying capabilities of actual worldwide forces.